Prof Dr Thomas Hoeren
Institute for Information, Telecommunications and Media Law
University of Münster

Lawyer Stefan Pinelli
Wolfsburg

Data law

Status: November 2024

Foreword

This book is intended to serve as an introduction to the gradually crystallising field of data law, building a bridge between academia and practice. Data law has developed rapidly since the publication of the European Digital and Data Strategy and is based on a large number of European legal acts aimed at regulating and controlling the use, exchange and security of data. The aim of this book is to provide a sound introduction to data law and, in particular, to help lawyers working in practice to navigate through the jungle of European legal acts.

The book is divided into three chapters. It begins with an introductory chapter on data law, in which we outline the cross-cutting issue of data law and explain the legal policy references to the Commission's digital and data strategy from 2020. The second chapter then deals in detail with the various data acts in the narrower sense. Here, we have taken inspiration from the bracket principle of the German Civil Code (BGB) and divided data law into a General Part and a Specific Part. The General Part consists of the horizontal legal acts such as the Data Act, the Data Governance Act and the GDPR – these regulations apply to all sector-specific legal acts, as the Union legislator regularly emphasises in the recitals to the various legal acts. The Specific part consists, among other things, of the sectoral legal acts such as the Regulation on the European Health Data Space (EHDS) or the Regulation on Access to Financial Data (FiDAR). This structuring of data law has not yet been presented in the literature in this form, and we hope to be able to enrich the still recent discussion on the systematisation of data law.

The third chapter deals with the European regulation of data-based business models. In our view, data-based business models are the common denominator of all legal acts that do not relate to data law in the narrower sense, but are nevertheless part of the overarching digital and data strategy and can be characterised as data law in the broader sense. When regulating data-based business models, the legislator pursues either a product-based approach, as seen in the AIA and the Cyber Resilience Act, or a function-based approach, which comes into play in the regulation of platforms through the Digital Services Act and the Digital Markets Act. The legislator's regulatory strategy is explained independently and supplemented with relevant examples and evidence.

The presentation of the individual legal acts follows a structured approach. After a brief introduction, we first outline the scope of each legal act and explain the respective rights and obligations of the parties involved. This is typically followed by a discussion on the supervision and enforcement of the regulations. Each section concludes with a summary and an examination of the practical implications. Throughout, we strived to emphasize issues of practical significance and, in some instances, propose potential solutions. Where feasible, we have included illustrations and diagrams to present the subject matter as clearly as possible.

Legislation, case law, and the continually expanding body of literature have been considered up to October 2024. All online sources were last accessed on 1 November 2024.

We extend our special thanks to the student assistants of the Civil Law Department at ITM Münster, whose active support has been instrumental in completing this work. We are particularly grateful to Martin Bangard, Ann-Cathrin Barth, Lando Derouaux, Madita Haustein, Fritz Heilmaier, Nicklas Hollas, Florian Holste, Maximilian Jaques, Vitus Kirchner, Friederike Reissenberger, Anna-Luise Rode, Yva Scheer, Pascal Schleking, Felix Schmidt-Rhaesa, Jillian Shepherd, Pascal Sonak, Tabea Süllwold, Ole Varwick, Wiebke Wahler, and Stella Wenzel for their invaluable assistance.

Finally, we express our heartfelt gratitude to Philip Mayer for his exceptional support, tireless dedication, and meticulous oversight in the organization, supervision, and continuous revision of this work.

We hope this publication proves insightful and thought-provoking, and we wish you an engaging reading experience.

Münster / Wolfsburg, November 2024

Thomas Hoeren / Stefan Pinelli

Table of contents

Chapter 1: Introduction to data law 13

I. Introduction 13

II. The European digital strategy as a legal policy turning point in data law 14

1. The European data strategy 14

a) Pillar 1: A cross-sector governance framework for data access and use 15

b) Pillar 2: Investment in data infrastructures and European capacities 16

c) Pillar 3: Strengthening data competences and skills 17

d) Pillar 4: Creation of common European data spaces 17

2. Evaluation 18

III. Data law - An attempt at systematisation 19

Chapter 2: Data law 21

A. General part of Data law 21

I. Data Act - Regulation (EU) 2023/2854 21

1. Introduction 24

2. Scope and definitions, Art. 1–2 DA 24

a) Territorial scope 25

b) Temporal scope 25

c) Material scope 25

d) Personal scope 33

3. Rights and obligations of data holders, users and data recipients 37

a) Introduction 37

b) Obligations of the data holder when using the data 38

c) Use of the data by users 42

d) Use by and provision of data to third parties 53

e) Dispute resolution by dispute resolution bodies (Art. 10 DA) 61

4. Unfair contract terms unilaterally imposed on another company , Art. 13 DA 63

a) Background 63

b) Scope of the clause control: B2B contracts 64

c) Abuse control 69
d) Legal consequences and enforcement 72
e) Practical recommendations 73
5. Provision of data to public authorities, the Commission, the European Central Bank and Union bodies on grounds of exceptional necessity, Art. 14–22 DA 74
a) Area 74
b) Requirement for data provision requests and prohibition of further use, Art. 17(1) – (3) DA 78
c) Fulfilment of data requests, Art. 18 DA 78
d) Obligations in handling the data received, Art. 19 DA 79
e) Compensation in the event of exceptional necessity, Art. 20 DA 80
6. Switching between data processing services, Art. 23–31 DA 81
a) Preliminary considerations and background to the regulation of data processing services 81
b) Data processing service, Art. 2 No. 8 DA 83
c) The switching process 86
d) Barriers to exchange, Art. 23 DA 90
e) Obligations for data processing services, Art. 23–31 DA 90
f) Gradual abolition of exchange fees, Art. 29 DA 97
g) Technical aspects of the bill of exchange, Art. 30 DA 99
h) Exceptions , Art. 31 DA 101
i) Sanctions and enforcement 102
7. Unlawful government access to and unlawful government transfer of non-personal data in an international context, Art. 32 DA 103
a) Background and area 103
b) Duty to prevent international transfer and access by government organisations, Art. 31(1) DA 104
c) Exceptions, Art. 31(2), (3) DA 104
8. Interoperability, Art. 33–36 DA 105
a) Overview and systematics 105
b) Interoperability of data rooms, Art. 33 DA 105

c) Interoperability for the parallel use of data processing services, Art. 34 DA 108
d) Interoperability of data processing services, Art. 35 DA 108
e) Smart Contracts, Art. 36 DA 109
9. Application and enforcement, Art. 37–42 DA 111
a) Competent authorities and data coordinators, Art. 37 DA 112
b) Right to lodge a complaint, Art. 38 DA 114
c) Right to an effective judicial remedy, Art. 39 DA 116
d) Sanctions, Art. 40 DA 116
e) Model contract clauses and standard contract clauses, Art. 41 DA 117
f) Role of the European Data Innovation Board (EDIB) Art. 42 DA 118
10. Databases containing certain data, Art. 43 DA 118
11. Final provisions, Art. 44–50 DA 119
12. Summary and implications for practice 119
II. The Relationship of the Data Act to the General Data Protection Regulation and Trade Secrets Protection Law 123
1. Introduction 124
2. Data Act and GDPR 125
a) Conflict between Data Act and GDPR for mixed data sets 125
b) Conflict of laws, Art. 1(5) DA 126
c) Personal roles 126
d) Access claims under Art. 4, 5 DA 128
e) Special categories of personal data pursuant to Art. 9 GDPR 133
f) Data access rights (Art. 4, 5 GDPR) and data portability (Art. 20 GDPR) 134
g) Legal basis for the processing of personal data in the context of data access claims pursuant to Art. 4, 5 DA and B2G data access pursuant to Art. 14 et seq. DA 134
h) Risk of fines 135
i) Conclusion 136
3. Data Act and trade secret protection law 136
a) Directive (EU) 2016/943 137
b) Relationship between the Directive (EU) 2016/943 and the Data Act 139

4. Summary and implications for practice 143
III. Legal framework for data governance under the Data Governance Act (DGA) - Regulation (EU) 2022/868 144
1. Introduction 145
a) Problem analysis of the status quo 146
b) Importance and function of data governance 147
c) Principles and systematics of the DGA 148
d) Demarcation of the DGA from the GDPR 149
2. Data held by public sector bodies, Art. 3–9 DGA 152
a) Sense and purpose of the regulations 152
b) Addressees of the provisions of the second chapter 153
c) No obligation of public sector bodies to disclose, Art. 1(2) DGA 154
d) Objectively recorded data and actions, Art. 3(1) DGA 155
e) Exclusion of certain types of data in Art. 3(2)(d),(e) DGA 158
f) Prohibition of exclusive arrangements, Art. 4 DGA 158
g) Conditions for re-use, Art. 5 DGA 159
h) Fees for re-use, Art. 6 DGA 163
i) Management of re-utilisation procedures, Art. 7, 8, 9 DGA 163
j) Criticism 164
3. Data intermediaries and data intermediation services 165
a) The term "data intermediation service", Art. 2 No. 11 DGA 165
b) Obligations of data intermediation services 171
c) Law enforcement 178
d) Criticism 180
4. Data altruism, Art. 16–25 DGA 182
a) Concept, function and principle of data altruism 182
b) National arrangements for data altruism, Art. 16 DGA 183
c) Recognised data altruism organisations, Art. 17–19 DGA 183
d) Transparency, protection and procedural requirements of data altruistic organisations, Art. 20–22, 25 DGA 185

e) Law enforcement: Competent authorities and monitoring practice, Art. 23, 24 DGA 187
5. Other regulations ... 187
a) The European Data Innovation Board, Art. 29 et seq. et DGA ... 187
b) International access and transfer, Art. 31 DGA ... 189
6. Supervision, enforcement and sanctions ... 190
7. Summary and practical implications ... 192
B. Specific part of Data law ... 195
I. Sector-specific data access regulations and the concept of European data spaces ... 195
II. European Health Data Space (EHDS) ... 199
1. Introduction ... 199
a) Legislative procedure ... 200
b) Goals ... 200
c) Structure and systematics of the EHDS ... 201
2. Rights and obligations of the parties involved ... 202
a) Primary use of electronic health data ... 202
b) Secondary use of electronic health data ... 203
3. Supervision , enforcement and sanctions ... 205
4. Summary and practical implications ... 206
III. Financial Data Access Regulation (FiDAR) ... 208
1. Introduction ... 208
2. Scope, Art. 2 FiDAR-D ... 209
3. Data access claims, Art. 4–7 FiDAR-D ... 211
a) Access by the customer, Art. 4 FiDAR-D ... 211
b) Access by a data user, Art. 5 (1) FiDAR-D ... 211
c) Authorisation dashboard, Art. 8 (1) FiDAR-D ... 212
4. Data sharing systems, Art. 9–11 FiDAR-D ... 212
5. Summary and practical implications ... 213
Chapter 3: Regulation of data-based business models ... 214
A. Product-related regulation ... 216
I. European cyber security law ... 219

1. Network and Information Security Directive (NIS) - Directive (EU) 2022/2555 219
a) Introduction 219
b) Scope, Art. 2 Directive (EU) 2022/2555 220
c) Obligations of covered entities, Art. 20 et seq. Directive (EU) 2022/2555 221
d) Supervision, enforcement and sanctions, Art. 31–37 Directive (EU) 2022/2555 224
e) Summary and practical implications 225
2. Cybersecurity Act (CSA) - Regulation (EU) 2019/881 (overview) 227
3. Cyber Resilience Act (CRA) – Regulation (EU) 2024/2847 229
a) Introduction 229
b) Interaction with other legal acts 231
c) Scope and definition 232
d) General provisions of the CRA 237
e) Rights and obligations of economic operators, Art. 13–26 CRA 241
f) Market surveillance, enforcement and sanctions 252
g) Summary and practical implications 254
4. Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 258
a) Preliminary considerations 258
b) Scope, Art. 2 DORA 260
c) Obligations for financial companies, Art. 5–35 DORA 261
d) ICT-related incidents - handling and reporting, Art. 17–19 DORA 267
e) Testing digital resilience through test programmes, Art. 24–27 DORA 267
f) Supervision, enforcement and sanctions, Art. 46 et seqq. DORA 269
g) Conclusion 270
II. Regulation on Artificial Intelligence - Regulation (EU) 2024/1689 272
1. Introduction 272
a) Background to the regulation of artificial intelligence 272
b) Objectives and recitals 273
c) Demarcations 274
2. Scope and definitions 275
a) Material scope 275

b) Personal scope 277
c) Territorial scope 277
d) Area exceptions 278
3. Rights and obligations 278
a) AI literacy, Art. 4 AIA 279
b) Prohibited AI practices, Art. 5 AIA 280
c) High-risk AI systems, Art. 6–49 AIA 281
d) Transparency obligations for providers and deployers of certain AI systems, Art. 50 AIA 289
e) AI models with a general purpose, Art. 51–56 AIA 292
4. Notifying authorities and notified bodies, Art. 28–39 AIA 296
5. Governance 296
a) Office for Artificial Intelligence (AI Office), Art. 64 AIA 297
b) AI Board (AI Board), Art. 65, 66 AIA 297
c) Market surveillance authority, Art. 3 No. 26 AIA 298
6. Sanctions 299
a) Fines 299
b) Further liability risks 300
c) Legal remedies 301
7. Summary and implications for practice 301
a) General criticism of the regulatory concept 301
b) In detail 302
c) Practical implications 304
B. Function-related regulation 305
IV. Platform-to-Business Regulation (P2BR) - Regulation (EU) 2019/1150 307
1. Introduction 307
a) Backgrounds 308
b) Goals 309
c) Differentiation from other legal acts of platform regulation 309
2. Scope, Art. 1(1), (2) P2BR 310

a) Personal scope ... 310
b) Material scope, Art. 2 P2BR ... 311
3. Requirements for online brokerage services and online search engines ... 316
a) Online brokerage services ... 316
b) Online search engines ... 325
4. Enforcement and supervision ... 326
a) Civil liability ... 327
b) Supervision, Art. 15 P2BR ... 328
c) Example Germany ... 328
5. Summary and implications for practice ... 328
V. Digital Service Act (DSA) - Regulation (EU) 2022/2065 ... 330
1. Introduction ... 331
a) Background and relationship to the E-Commerce Directive, Art. 2, 89 DSA ... 331
b) Legal policy considerations ... 332
c) Concrete goals ... 333
d) Basic structure ... 334
2. Area ... 335
a) Material-personal scope ... 335
b) Territorial scope (market place principle), Art. 2(1) DSA ... 340
3. (Due diligence) obligations and liability of providers of intermediary services, Art. 4–48 DSA ... 342
a) General liability ng concept, Art. 4–6 DSA ... 342
b) No general obligation to monitor or actively investigate, Art. 8 DSA ... 347
c) Judicial and official orders, Art. 9–10 DSA ... 347
d) Due diligence and transparency obligations for brokerage services ... 348
4. Supervision and enforcement, Art. 49–63 DSA ... 374
a) Supervision and enforcement by the Member States, Art. 49–55 DSA ... 375
b) Compensation Art. 54 DSA ... 376
c) Coordinated investigations and coherence mechanisms, Art. 57 DSA ... 377
d) European Digital Services Board, Art. 61–63 DSA ... 378

e) Enforcement of obligations of providers of very large online platforms and very large online search engines ... 379
5. Summary and implications for practice ... 383
VI. Digital Markets Act (DMA) - Regulation (EU) 2022/1925 ... 386
1. Introduction ... 387
a) Economic background of the DMA ... 387
b) Objectives of the DMA ... 388
c) Relationship to European and national competition law ... 389
d) Relationship to the Digital Services Act ... 390
2. Material and territorial scope, Art. 1(2) DMA ... 391
b) Appointment as gatekeeper, Art. 3 DMA ... 392
3. Obligations of the gatekeepers ... 394
a) Duty to cooperate, Art. 3(3) DMA ... 394
b) Duties of conduct and omission, Art. 5–7 DMA ... 394
c) Obligations of gatekeepers in accordance with Art. 5 DMA ... 395
d) Obligations of gatekeepers in accordance with Art. 6 DMA ... 401
4. Supervision and enforcement, Art. 20–43 DMA ... 408
b) Sanction options, Art. 20 et seqq. DMA ... 409
c) Private enforcement ... 411
5. Summary and implications for practice ... 413
a) Criticism regarding the appointment of gatekeepers ... 414
b) Criticism regarding the prohibition of data merging (Art. 5(2) DMA) ... 416
c) Outlook ... 416

Chapter 1: Introduction to data law

Bibliography

Apel, S., & Huber, C., "Das neue Datenrecht der EU – eine Übersicht," *JuS* (2024), 410; Apel, S., & Huber, C., "Das neue Datenrecht der EU – eine Übersicht," *JuS* (2024), 514; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Data Strategy, COM(2020) 66 final; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Shaping Europe's Digital Future, COM(2020) 67 final; Hennemann, M., & Steinrötter, B., "Der Data Act," *NJW* (2024), 1; International Data Corporation (IDC), The Digitization of the World – From Edge to Core, *2018*, accessible at: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf; Podszun, R., "Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks," 2023; Neuner, J., Allgemeiner Teil des Bürgerlichen Rechts, 13th ed., C.H. Beck 2023; Schmidt-Kessel, M., & Bomhard, D., *MMR* (2024), 69; Schmitz, T., "Digitale-Gesetze-Strategie – Agilität oder 'Act'ionismus?" *ZD* (2022), 189; Schreiber, K., Pommerening, P., & Schoel, P., *Das neue Recht der Daten-Governance – Data Governance Act (DGA)*, 1st ed., Nomos 2022; Schreiber, K., Pommerening, P., & Schoel, P., *Der neue Data Act*, 2nd ed., Nomos 2024; Specht, L., & Hennemann, M. (eds.), Data Governance Act, 1st ed., Nomos 2023; Specht-Riemenschneider, L., "Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO," *ZEuP* (2023), 638; Specht-Riemenschneider, L., Werry, N., & Werry, S. (eds.), Datenrecht in der Digitalisierung, 1st ed., Erich Schmidt Verlag 2019; Wolff, H. A., Brink, S., & v. Ungern-Sternberg, A. (eds.), Beck'scher Online-Kommentar Datenschutzrecht, 49th ed., Status: 1 August 2024, C.H. Beck.

I. Introduction

This script provides an introduction to the legal field of **data law**. But what lies behind this colourful term? Data law refers to the totality of all standards that regulate the access, use and protection of data, regardless of whether it is personal or non-personal data. It is a classic cross-sectional subject with borrowings from various areas of law such as antitrust law, competition law and consumer protection law.[1] The best-known sub-area of data law to date is probably data protection law, which has undergone significant further development with the introduction of the General Data Protection Regulation (GDPR) in 2017.[2] At the same time, the technology underlying the generation and processing of data has developed rapidly. One example of this is the major progress made in the field of artificial intelligence, which has moved to the centre of social debate thanks to chatbots such as 'ChatGPT'. No less dynamic is the technical development in the area of the Internet of Things (IoT), which has produced a large number of products connected to the Internet, such as smartphones, smartwatches and smart home assistants, whose use has become a matter of course in consumers' everyday lives. The technological progress of the information society goes hand in hand with the growth in the amount of data generated. By way of

1 Specht-Riemenschneider, L./Werry, N./Werry, S., Datenrecht in der Digitalisierung, p. 5; Apel, S./Huber, C., *JuS* 2024, 410, (410).

2 Apel, S./Huber, C., *JuS* 2024 410, (410).

comparison, while 33 zettabytes of data were generated worldwide in 2018, this figure is expected to rise to 175 zettabytes by 2025, or the equivalent of 175,000,000,000,000 gigabytes.[3] This data harbours considerable potential for value creation, as it can be used for the further development and improvement of connected products on the secondary market.[4] However, the reality paints a different picture: a study commissioned by the European Commission has shown that the economic potential of data is currently not being fully utilised, as an estimated 80% of industrial data remains unused.[5]

II. The European digital strategy as a legal policy turning point in data law

The European Commission has recognised this imbalance and, with the presentation of the **digital strategy** in February 2020, has set the political course for a "fundamental social change"[6] , which redefines the fundamental importance of data in the economic, social and political spheres. The digital strategy is a comprehensive strategic concept for shaping Europe's digital future, comprising a total of over 50 key measures.[7] The aim is to develop and deploy trustworthy technologies that improve the everyday lives of European citizens without undermining European values. The Commission is also endeavouring to promote a fair and competitive economy that is strengthened by digital innovations and guarantees comprehensive consumer protection. It also aims to support an open, democratic and sustainable society in which digital technologies contribute to upholding and strengthening democratic values and fundamental rights.[8]

To realise these goals, the Commission has defined a series of measures aimed at expanding digital infrastructures, strengthening cyber security and promoting digital skills.[9] The digital strategy also addresses the dark sides of the digital economy. These include, above all, the market power of large (tech) companies, which the Commission believes needs to be curbed, and the lack of access to data for a large number of market participants, which makes it almost impossible to share data.[10]

1. The European data strategy

A key measure on the path to a fair and competitive economy is the **European data strategy**, which aims to give Europe a "global leadership role in the data-agile economy"[11].[12] The data strategy aims to create a European data economy by 2025 that is efficient, innovative and closely aligned with European values and fundamental rights.[13] At the centre of this strategy is the idea of a **European data space** in

3 IDC, The Digitisation of the World, p. 3.
4 Cf. Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, p. 10.
5 https://ec.europa.eu/commission/presscorner/detail/de/ip_22_1113.
6 COM(2020) 67 final, p. 1.
7 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 1 para. 19.
8 COM(2020) 67 final, p. 3, 17.
9 COM(2020) 67 final, p. 8.
10 COM(2020) 67 final, p. 10; COM(2020) 66 final, p. 9.
11 COM(2020) 67 final, p. 11.
12 COM(2020) 67 final, p. 11.
13 COM(2020) 66 final, p. 2 et seqq.

the sense of a **common internal market for data**, in which both personal and non-personal data can be made accessible and used under predefined conditions.[14]

The European Union is currently still a long way from the ideal of a European data space, as the Commission states in its data strategy.[15] A number of problems have been identified in this regard: a central problem is the **fragmentation of the internal market** due to different and in some cases non-existent regulations in the Member States regarding the access and use of data. While some Member States already have corresponding laws, other Member States lack such regulations.[16] The resulting legal uncertainty and the **different levels of cyber security** in the European Union lead to a lack of trust in the (voluntary) sharing of data both between companies and between companies and public authorities or private individuals.[17] Regardless of the legal framework, the **lack of availability of data** is another fundamental problem. Although more and more data is being generated, it is often not available to a sufficient extent for the (economic) players involved, especially in the private sector.[18] One reason for this and another problem, is the **power imbalance** between large platform companies on the one hand and smaller companies such as SMEs on the other.[19] As a rule, platform companies already have considerable amounts of data at their disposal due to their business model, which gives them a competitive advantage over less data-rich market participants who have little or no access to such data. In addition, the **quality and interoperability** of the sporadically available data is often inadequate, which may represent an insurmountable hurdle for companies operating in the same sector, but at the very least massively impairs the cross-sector utilisation of data.[20] Last but not least, the European Economic Area also lacks the **data expertise** required to prepare and analyse data, as making data accessible alone does not bring any benefits for companies.[21] Appropriately qualified specialists are always needed to be able to draw the right conclusions from the data for companies.

For its part, the data strategy is based on four pillars, all of which are aimed at overcoming the aforementioned problems in the internal market through targeted measures.

a) Pillar 1: A cross-sector governance framework for data access and use

The first pillar consists of a horizontal legal framework for data access and use in the European Union to ensure that data can be used across sectors and in a harmonised manner throughout Europe.[22] With the **Data Governance Act**, which came into force on 23 June 2022, the European legislator has put its

14 COM(2020) 67 final, p. 9; COM(2020) 66 final, p. 5 et seq.
15 COM(2020) 66 final, p. 7 et seq.
16 COM(2020) 66 final, p. 7 with further references.
17 COM(2020) 66 final, p. 8, 13.
18 COM(2020) 66 final, p. 7 et seqq.
19 COM(2020) 66 final, p. 9.
20 COM(2020) 66 final, p. 10.
21 COM(2020) 66 final, p. 12.
22 COM(2020) 66 final, p. 14.

words into action and launched a uniform governance framework for the voluntary sharing[23] of data and, in particular, for the reuse of data held by public sector bodies.[24]

In order to improve the quality and availability of public sector data, the Commission has also adopted the implementing regulation on high-quality datasets provided for in Art. 14(1) of the PSR Directive. The regulation has been applicable since 9 June 2024 and defines the list of high-quality datasets belonging thematically to the categories of geospatial, earth observation, environment, meteorology, statistics, companies and ownership of companies and mobility, and prescribes quality standards. Data held by public authorities must now be published by the Member States under free licences.

What was still cautiously announced in the data strategy as a Commission review mandate can now be described as the centrepiece of the European data economy.[25] We are talking about the Data Act, which came into force on 11 January 2024. The Data Act is to be understood as a comprehensive horizontal regulatory framework that - like the Data Governance Act - applies to all sectors and whose core element is the right of access to data from connected products and related services.[26]

Finally, as part of Pillar 1, the Commission plans to set up data pools through appropriate measures to provide data for corresponding analyses and machine learning. The Data Act is also linked to the announced revision of competition law guidelines with relevant stakeholders and the review of the consequences of data accumulation as a result of company acquisitions. Finally, the Commission vows to make greater use of data-based decision-making in politics in order to set a good example.

While the provisions of the Data Governance Act and the Data Act are intended to counteract the problem of legal fragmentation of the internal market, the implementing regulation on high-quality datasets addresses the problem of insufficient data quality, even though the regulation only relates to data held by public bodies.

b) Pillar 2: Investment in data infrastructures and European capacities

The second pillar of the data strategy focuses increasingly on the technical infrastructure required for the digital transformation and data-based business models. The massive amounts of data that will be processed, stored and used in the future will require investment in cloud and computing infrastructure.[27] Specifically, this includes public investment in decentralised computing capacities (edge computing), high-performance computing, quantum computing, cyber security, low-power processors and 6G networks.[28] In particular, the aim is to create the technical conditions for an interoperable European data space. The flagship project is the High-Impact Project, which aims to mobilise total investment of 4 - 6

[23] On so-called data altruism, see III. 4.
[24] For the Data Governance Act, see Section III.
[25] Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, p. 19, speaks in this respect of the "Basic Law of the Data Economy".
[26] Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, p. 9.
[27] COM(2020) 66 final, p. 18 et seq.
[28] COM(2020) 66 final, p. 19.

billion euros, of which around two billion will be contributed by the Commission. As part of the High Impact Project, the member states are to come together for the purpose of a cloud merger and, among other things, create synergy effects with the 'Gaia-X project'.[29]

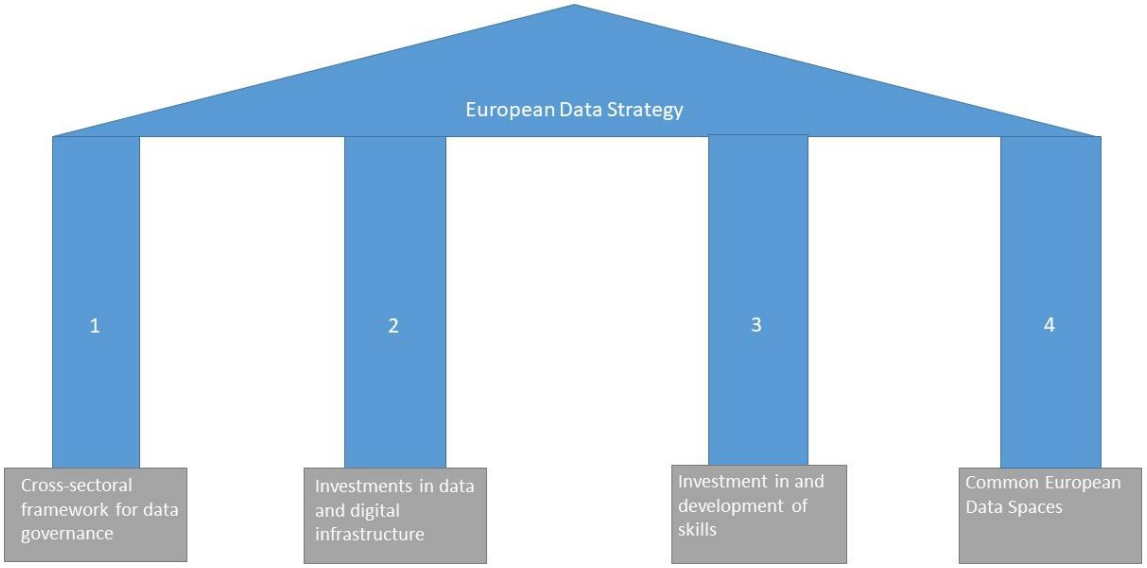
c) Pillar 3: Strengthening data competences and skills

The third pillar of the data strategy aims to strengthen the competences of EU citizens and companies in dealing with data.[30] This is not just about improving technical expertise in the sense of educational measures, but also about improving the data sovereignty of individuals by giving them more control and decision-making power over their data.[31] This concern is expressed in the review mandate, which is referred to as a key measure, according to which the Commission is considering the extension of the right to data portability standardised in Art. 20 GDPR.[32] The shortage of skilled labour in the digital sector, on the other hand, is to be overcome by giving greater consideration to women and through technological progress in the area of big data and learning analytics.[33]

d) Pillar 4: Creation of common European data spaces

The final pillar of the strategy relates to the creation of sector-specific European data spaces in strategically important areas such as health, mobility, energy and agriculture.[34] The common European data spaces are intended to improve the availability of data in the respective sectors and facilitate the exchange of data between public and private stakeholders. As a result, the Commission hopes that the establishment of data spaces will strengthen innovation in the relevant sectors for the common good.[35] One example is the planned European Health Data Space, which is intended to promote the secure exchange of health data between researchers, clinics and patients.[36]

[29] COM(2020) 66 final, p. 21.
[30] COM(2020) 66 final, p. 23.
[31] COM(2020) 66 final, p. 23.
[32] COM(2020) 66 final, p. 25.
[33] COM(2020) 66 final, p. 24.
[34] COM(2020) 66 final, p. 25 et seq.
[35] COM(2020) 66 final, p. 8, 28.
[36] COM(2020) 66 final, p. 34.



Source: Own illustration

2. Evaluation

The political endeavours of the European Data Strategy mark an overdue **change of course in data law**, as they place a clear focus on the use of data for the first time, instead of focusing exclusively on the protection of personal data as has been the case to date - the Commission is thus restoring the balance between the overemphasis on the protection of privacy and the commercial use of data since the GDPR came into force.[37] While harmonised EU data protection law aims to minimise the processing of personal data through the principle of prohibition, the data strategy rightly emphasises the **economic value and innovation potential** of data, which exists regardless of the personal nature of the data. This realisation leads to a shift away from a purely restrictive perspective towards a balanced view that promotes the **free flow of data** within the internal market without tearing down the walls of data protection that have been erected. The extent to which the individual key measures actually pave the way for a common internal market for data cannot be conclusively assessed here. From today's perspective, however, the digital strategy can rightly be described as a turning point in data law in terms of legal policy, in view of the numerous European legal acts adopted in recent years.

[37] See also Schmitz, T., *ZD* 2022, 189 (190).

III. Data law - An attempt at systematisation

Based on the division of the Union legislator into horizontal and sectoral legal acts, data law can be subdivided into a **general part** and a **specific part.** The general part comprises the horizontal legal acts that apply to all types of data and their use across all sectors.[38] The horizontal provisions are thus, so to speak, drawn in front of the parenthesis and also apply to the sectoral legal acts, unless otherwise stipulated.[39] The horizontal legal acts of the General Part include, above all, the Data Act, the Data Governance Act and the provisions of the GDPR. In contrast, the Specific Part of data law includes legal acts aimed at regulating certain categories or sectors of data.[40] Recent examples that should be mentioned here in particular include the Commission's proposals for a regulation on the European Health Data Space[41] and the proposal for a regulation on a framework for access to financial data[42]. In addition, the sector-specific regulations[43] that already applied before the adoption of the data strategy are also covered by the special section of data law. These include, in particular, the provisions of the PSI Directive[44] , the ITS Directive[45] , the Payment Services Directive[46] , the Electricity[47] and Gas Directives, the Type Approval and Vehicle Emissions Regulation[48] and the General Data Protection Regulation[49]. What all legal acts have in common is that they contain regulations on the collection, access or use of certain data

38 Rec. 42 Regulation (EU) 2023/2854; Rec. 3 Regulation (EU) 2022/868; Schreiber, K./Pommerning, P./Schoel, P., Der neue Data Act, § 3 para. 34 speak instead of a "symmetrical regulatory approach".

39 The principle of brackets is also found in the General Part of the German Civil Code and serves to systematise and avoid contradictions in value. For more details, see Neuner, J., Allgemeiner Teil des Bürgerlichen Rechts, § 7 para. 12 et seq.

40 Schreiber, K./Pommerning, P./Schoel, P., Der neue Data Act, § 3 para. 34 use the term asymmetric regulation for this.

41 COM(2022) 97 final; See also the Commission's press release on the adoption of the text of the Regulation by the European Parliament of 24 April 2024 https://ec.europa.eu/commission/presscorner/detail/de/ip_24_2250.

42 COM(2023) 360 final.

43 See the list of sector-specific legislation in the Data Strategy, COM(2020) 66 final, p. 4 et seq.

44 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56–83.

45 Directive (EU) 2010/40 of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJ L 207, 6.8.2010.

46 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L, No 337, 23.12.2015, p. 35–127.

47 Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, OJ L 158, 14.6.2019, p. 125.

48 Regulation (EU) 2024/1257 of the European Parliament and of the Council of 24 April 2024 on type-approval of motor vehicles and engines and of systems, components and separate technical units intended for such vehicles, with respect to their emissions and battery durability (Euro 7), amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 715/2007 and (EC) No 595/2009 of the European Parliament and of the Council, Commission Regulation (EU) No 582/2011, Commission Regulation (EU) 2017/1151, Commission Regulation (EU) 2017/2400 and Commission Implementing Regulation (EU) 2022/1362, OJ L, 8.5.2024.

49 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59.

in a specific sector. These sector-specific standards apply in addition to the general rules of data law and take account of the particularities of each sector.

For the application of the law, this subdivision of data law means that in the absence of sectoral provisions on a specific issue, the corresponding provisions of the horizontal legal acts can be used. For example, the horizontal provisions on consideration for the provision of data pursuant to Art. 9(2) DA should apply equally to the determination of remuneration pursuant to Art. 5(2) FiDAR.[50] The application of horizontal provisions in the context of data exchange on the basis of sectoral provisions is sometimes expressly ordered by the legislator.[51] If the application of horizontal provisions is not expressly prescribed in the sectoral legislation, a case-by-case examination of the respective provisions is always required.

Data law in a broader sense also includes a number of other legal acts that do not directly regulate data, but also affect other areas of law. Although the NIS 2 Directive, the Cyber Security Act and the Cyber Resilience Act are primarily aimed at product-specific or functional cybersecurity standards, they share the overarching goal of protecting data in digital infrastructures and thus strengthening trust in the internal market. The Digital Markets Act and the Digital Services Act also address data-related issues by establishing market rules for large digital platforms whose core business model includes the collection and processing of a large amount of (user) data. Also inextricably linked to the processing of data is the provision of AI models, which the European legislator intends to regulate with the Artificial Intelligence Regulation adopted in June 2024.

The lecture notes take up this tripartite division of data law: In the first part, the basic regulations of data law AT are presented, consisting of the Data Act and the Data Governance Act. The second part deals with sector-specific data law, which for capacity reasons is limited to the more recent legal acts in the area of European data spaces. Finally, Chapter 3 presents the legal acts on European cybersecurity law, the regulation of artificial intelligence and platform regulation under the heading of data-based business models.

---

50 COM(2023) 360 final, p. 9.

51 See Rec. 47 FiDAR-D: The proposal for a Data Act [Regulation (EU) XX] establishes a horizontal framework for access to and use of data across the Union. This Regulation complements and specifies the rules laid down in the proposal for a Data Act [Regulation (EU) XX] Therefore those rules also apply to the sharing of data governed by this Regulation. This includes provisions on the conditions under which data holders make data available to data recipients, on compensation, dispute settlement bodies to facilitate agreements between data sharing parties, technical protection measures, international access and transfer of data and on authorised use or disclosure of data.

Chapter 2: Data law

A. General part of Data law

I. Data Act - Regulation (EU) 2023/2854

Bibliography

Alpaydin, E., Maschinelles Lernen, 3rd ed., De Gruyter 2022; Antoine, L., "Datenzugang im Spannungsfeld zwischen DS-GVO, Geschäftsgeheimnisschutz und Datenbankherstellerrecht," *CR* (2024), 73; Antoine, L., "Datenzugangsrechte im finalen Data Act - Fortschritt, Rückschritt, neue Fragen? Schlüssel zur Förderung datengetriebener Geschäftsmodelle," *CR* (2024), 1; Assion, S., & Willecke, L., "Der EU Data Act – Die neuen Regelungen zu vernetzten Produkten und Diensten," *MMR* (2023), 805; Beinke, L., & Daute, I., "Der Fairnesstest des Data Act," *RDi* (2024), 69; Bomhard, D., "Auswirkungen des Data Act auf die Geschäftsmodelle von Cloud-Anbietern," *MMR* (2024), 109; Bomhard, D., "Der Anwendungsbereich des Data Act," *MMR* (2024), 71; Bomhard, D., "Der EU Data Act – Neuer Rechtsrahmen für die Datenwirtschaft," *GmbHR* (2022), Heft 14, R212; Bomhard, D., & Merkle, M., "Der Entwurf eines EU Data Acts," *RDi* (2022), 168; Borges, G., "Smart Contracts für Datentransaktionen und der Data Act," *CR* (2024), 425; Danyeli, G., "Die grosse Freiheit über die Wolke? Die Regelungen des Data Act zum Wechsel von Cloud-Anbietern und zur Interoperabilität," *DSRITB* (2022), 427; Deutscher Anwaltverein (DAV), "Stellungnahme des Deutschen Anwaltvereins zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für fairen Datenzugang und Datennutzung (Data Act)", accessible at: https://anwaltverein.de/de/newsroom/sn-40-22-vorschlag-der-eu-kommission-fuer-ein-datengesetz; Deutscher Industrie- und Handelskammertag (DIHK), "Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für fairen Datenzugang und Datennutzung (Data Act)", May 2022, accessible at: https://www.dihk.de/resource/blob/71822/4a99bc6537af818d2e5c456f0879dc95/dihk-stellungnahme-data-act-data.pdf, J., Banda, O., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, V., Moscon, V., Richter, H., & Wiedemann, K., "Position Statement of the Max Planck Institute for Innovation and Competition on the Proposal for harmonised rules on fair access to and use of data (Data Act)", abrufbar unter: https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content; Ehlen, T., & Sebulke, P., "Der Data Act – Zwischen Markt- und Vertragsgestaltung," *CR* (2024), 84; Ehmann, E., & Selmayr, M. (eds.), Datenschutz-Grundverordnung, 3rd ed., C.H. Beck 2024; Etzkorn, P., "(Vertragliche) Datenzugangsansprüche nach dem Data Act," *RDi* (2024), 116; European Commission, Datengesetz – Factsheet, 2022, accessible at: https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet; European Commission, Frequently Asked Questions Data Act, accessible at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act; European Commission, Impact Assessment Report – Accompanying the Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act), SWD(2022) 34 final; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, COM(2020) 66 final; Fries, M., & Paal, B., Smart Contracts, Mohr Siebeck 2019; Funk, A., "Das Prinzip der Nutzerzentriertheit des Data Act – ein gravierender Strukturfehler," *CR* (2023), 421; Gerpott, T., "Vorschlag für ein europäisches Datengesetz – Überblick und Analyse der Vorgaben für vernetzte Produkte," *CR* (2022), 271; Hartl, K., & Vogel, P., "Data Act und Legal Tech," *LTZ* (2024), 104; Hayward, A., Mironescu, D., Cattaneo, F., Aguzzi, S., van der Wees, C., Stefanatou,

D., & van Sleen, C., "Switching of Cloud Services Providers", 2018, accessible at: https://op.europa.eu/en/publication-detail/-/publication/799e50ff-6480-11e8-ab9c-01aa75ed71a1/language-en;
Heinzke, P., "Data Act: Auf dem Weg zur europäischen Datenwirtschaft," *BB* (2023), 201; Heinzke, P., "Data Act: Ein neuer Baustein des europäischen Datenrechts," *GRUR-Prax* (2023), 154; Heinzke, P., "Data Act: Neue Regeln für Cloud-Service-Provider," *BB* (2023), 1291.
Heinzke, P., Herbers, B., & Kraus, M., "Datenzugangsansprüche nach dem Data Act," *BB* (2024), 649; Hennemann, M., Ebner, G., Karsten, L., Lienemann, G., & Wienroeder, M., Data Act – An Introduction, 1st ed., Nomos 2024; Hennemann, M., & Sattler, A. (eds.), Immaterialgüter und Digitalisierung, Nomos 2018; Hennemann, M., & Steinrötter, B., "Data Act – Fundament eines neuen EU-Datenwirtschaftsrechts," *NJW* (2022), 1481; Hennemann, M., & Steinrötter, B., "Der Data Act – Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen," *NJW* (2024), 1; Herrmann, P., & Schlingloff, J. (eds.), Münchener Kommentar zum Lauterkeitsrecht, Band 2, 3rd ed.,C.H. Beck 2022; Hoeren, T., "Alibaba und das Dateneigentum – 25 Jahre später," *MMR* (2023), 32; Hoeren, T., & Pinelli, S. (eds.), IT-Vertragsrecht, 4th ed., De Gruyter 2024; Hoeren, T., Sieber, U., & Holznagel, B. (eds.), Handbuch Multimedia-Recht, 62nd ed., C.H. Beck 2024; Holznagel, B., & Freese, F., "EU Data Act: Ein wichtiger Baustein in der Europäischen Datenstrategie," *EuZ* (2023), A 1 – 34; Jung, S., "Die Missbrauchskontrolle von Vertragsklauseln nach Art. 13 Data Act," *ZIP* (2024), 1565; Kaesling, K., "B2B- und B2C-Datennutzung nach dem Data Act," *GRUR* (2024), 821; Karsten, L., & Wienroeder, M., "Der Entwurf des Data Act – Auswirkungen auf die Automobilindustrie," *RAW* (2022), 99; Kaulartz, M., & Heckmann, D., "Smart Contracts – Anwendungen der Blockchain-Technologie,"*CR* (2016), 618; Keller, E., Schönknecht, M., & Glinke, A. (eds.), Geschäftsgeheimnisschutzgesetz, Beck'sche Kurz-Kommentare, 1st ed., C.H. Beck 2021; Keppeler, L., Schneider, R., & Nickel, A., "Der Dateninhaber im Data Act – faktische Datenherrschaft als Ausweg aus der Definitionsmisere des Art. 2 Nr. 13 DA," *ITRB* (2024), 180; Kerber, W., "EU Data Act: Will new user access and sharing rights on IoT data help competition and innovation?" *JoAE* (2024), 1; Kerber, W., "Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives," *GRUR Int.* (2023), 120; Kim, D., "Der Datenbankschutz sui generis nach dem Data Act," *MMR* (2024), 87; Kipker, D., Birreck, P., Niewöhner, M., & Schnorr, T., "Rechtliche und technische Rahmenbedingungen der 'Smart Contracts' – Eine zivilrechtliche Betrachtung," *MMR* (2020), 509; Köhler, H., Bornkamm, J., & Feddersen, C. (eds.), Gesetz gegen den unlauteren Wettbewerb, 14th ed., Band 13a, C.H. Beck 2024; Krämer, J., "Improving the effectiveness of the B2B and B2C data sharing obligations in the proposed Data Act," *CERRE Report*, November 2022; Lagoni, J., "Cloud Switching gemäß Data Act: Die Abschaffung von Switching Charges," *CR* (2024), 91; Leeb, M., & Liebhaber, A., "Grundlagen des Datenschutzrechts," *JuS* (2018), 534; Lettl, T., "Rechtsfolgen der Missbräuchlichkeit einer Vertragsklausel nach Art. 6 Abs. 1 RL 93/13/EWG (Klausel-RL) und Art. 13 Abs. 1, 7 VO (EU) 2023/2854 (Datenverordnung oder Data-Act)," *WM* (2024), 185; Lorenzen, B., "Geschäftsgeheimnisschutz und Data Act," *Zeitschrift für geistiges Eigentum (ZGE)* (2022), 250; Martens, B., Methodenlehre des Unionsrechts, Mohr Siebeck 2013; Martens, B., Parker, G., Petropoulos, G., & Van Alstyne, M., "Towards Efficient Information Sharing in Network Markets," *TILEC DP 2021014*, accessible at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3956256; McGuire, R., & Schulte-Nölke, H., "Ansprüche des Nutzers gegen den Dateninhaber nach dem Data Act," *ZdiW* (2024), 73; McKinsey & Company, *The Internet of Things: Catching up to an accelerating opportunity*, 2021, accessible at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it#/; Metzger, A., Schweitzer, H., & Wagner, G., "Datenschutz und Datenmarkt: Grundzüge einer Marktordnung für die europäische Datenwirtschaft," *ZfPW* (2023), 227; Metzger, A., & Schweitzer, H., "Shaping Markets: A Critical Evaluation of the Draft Data Act," *ZEuP* (2023), 42; Möslein, F., Dispositives Recht, Mohr Siebeck 2011; Müller, J., "Der Schutz faktischer Kontrolle durch die Rechtsordnung," *RDi* (2024), 297; Niedermaier, T., & Picht, P., "'Halbstarke' als Friedensstifter – alternative

Streitbeilegung im Data Act und der SEP-Verordnung," *EuZW* (2023), 1035; Ohly, A., "Das neue Geschäftsgeheimnisgesetz im Überblick," *GRUR* (2019), 442; Niehaus, M., & Siems, J., "Welche Daten fallen unter die Zugangs- und Weitergabeansprüche des EU Data Act? Eine Analyse des Anspruchsgegenstands," *ZdiW* (2024), 50; Oster, J., "Nach der 'Batterie-Mietbedingungen' Entscheidung: Wie geht es weiter mit Smart Contracts?" *ZfPW* (2023), 387; Otto, B., Steinbuß, S., Teuscher, C., & Lohmann, C., Reference Architecture Model, Version 3.0, 2019, accessible at: https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf; Paal, B., & Fenik, M., "Access to Data in the Data Act Proposal," *ZfDR* (2023), 249; Paulus, D., "Was ist eigentlich … ein Smart Contract?" *JuS* (2020), 107; Pauly, D.A., Wichert, F., & Baumann, J., "Schutz von Geschäftsgeheimnissen nach dem Data Act," *MMR* (2024), 211; Pertot, T., *Rechte an Daten*, Mohr Siebeck 2020; Picht, P.G., "Caugh in the Acts – Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law," *MPI Research Paper No. 22-12*; Piltz, C., & Zwerschke, J., "Cloud Switching nach dem Data Act aus der Beratungsperspektive," *CR* (2024), 153; Podszun, R., & Pfeifer, C., "Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission," *GRUR* (2022), 953; erening, P., & Nickel, M., "Wechsel zwischen Datenverarbeitungsdiensten nach dem Data Act – Eine Herausforderung für die Vertragspraxis," *RDi* (2024), 289; Redeker, H. (eds.), Handbuch IT-Verträge, 52nd ed. 03/2024; Remke, C., "Rechtsdurchsetzung unter dem Data Act," *MMR* (2024), 117; Riesenhuber, K., Europäische Methodenlehre, 4th ed., De Gruyter 2021; Säcker, F.J., Rixecker, A., Oetker, H., & Limperg, S. (eds.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2, 9th ed., C.H. Beck 2022; Sattler, A., "Anbieterwechsel nach dem Data Act – Standardvertragsklauseln für Verträge über Cloud-Computing," *CR* (2024), 213; Jidt-Kessel, M., "Heraus- und Weitergabe von IoT-Gerätedaten," *MMR* (2024), 75; Schmidt-Kessel, M., "Zahlungsverzug im Handelsverkehr – ein neuer Richtlinienentwurf," *JZ* (1998), 1135; Schreiber, K., "Revolutioniert der Data Act die Datenwirtschaft?" *MMR* (2023), 541; Schreiber, K., Pommerening, P., & Schoel, P., *Der neue Data Act – mit Data Governance Act*, 2nd ed., Nomos 2024; Schröder, M., "Bereitstellung von Daten wegen außergewöhnlicher Notwendigkeit," *MMR* (2024), 104; Schwamberger, S., "Die Klauselkontrolle in Art. 13 Data Act," *MMR* (2024), 96; Siglmüller, J., "Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft," *MMR* (2024), 112; Specht, L., & Henneman, M. (eds.), Data Governance-Act, Handkommentar, 1st ed., Nomos 2023; Specht-Riemenschneider, L., "Der Entwurf des Data Act," *MMR* (2022), 809; Staudenmayer, D., "Der Data Act im Gefüge des europäischen digitalen Privatrechts," *NJW* (2024), 1377; Steinrötter, B., "Verhältnis von Data Act und DS-GVO," *GRUR* (2023), 216; Stempel, C., Treu und Glauben im Unionsprivatrecht, Mohr Siebeck 2016; Weinhold, R., & Schröder, C., "(R)Evolution oder vergebene Chance?" *ZD* (2024), 306; Weiß, R., "Streitbeilegung nach Art. 10 Data Act," *MMR* (2024), 101; Wentzel, C., & Lutz, B., "Zugangsanspruch zu Reparatur- und Wartungsinformationen nach der Typengenehmigungsverordnung und Data Act – Eine Gegenüberstellung," *RAW* (2024), 123; v. Westphalen, F., "Der neue Data Act – Eine Kaskade AGB-rechtlicher Verbote im unternehmerischen Verkehr," *BB* (2024), 515; v. Westphalen, F., Thüsing, G., & Pamp, J. (eds.), Vertragsrecht und AGB-Klauselwerke, 50th ed., C.H. Beck 2024; Wiebe, A., "Der Data Act als vertragsrechtlicher Rahmen für Datennutzungsvorgänge – Anwendungsbereich und Vorhaben der Missbrauchskontrolle nach Art. 13 Data Act-E," *CR* (2023), 777; Wiebe, A., "Der Data Act – Innovation oder Illusion?" *GRUR* (2023), 1569; Wiedemann, N., Conrad, T., & Salemi, S., "Bereitstellung von Daten nach dem Data Act – offene Fragen und verbleibende Probleme," *K&R* (2024), 157; Wilken, T., & Rammos, T., "Der Data Act – Chancen und Risiken für Unternehmen durch das geplante europäische Datengesetz," *DB* (2022), 1241; Wilkening, P., & Müller, J., "Data Act – Neue Datenzugangs- und Datennutzungsregeln für die Daten- und Cloudwirtschaft," *DB* (2024), 166; Witzel, M., "Der Entwurf des Data Act und seine Vorgaben an die Vertragsgestaltung," *CR* (2022), 561; Wolff, H. A., Brink,

S., & v. Ungern-Sternberg, A. (eds.), Beck'scher Online-Kommentar Datenschutzrecht, 49th ed., Status: 1 August 2024, C.H. Beck.

1. Introduction

The *Internet of Things* (IoT) is the infrastructural cornerstone of the digital economy, as it enables the generation of large amounts of data through the networking of physical and virtual objects, which in turn form the basis for data-driven business models, innovative services and a more efficient use of resources. For the European domestic market, the data streams generated by IoT technologies mean enormous potential for value creation: it is estimated that the value of IoT-related products and services could be between 5.5 and 12.6 trillion US dollars worldwide by 2030.[52] Nevertheless, up to 80% of IoT data remains unutilised as access to data is often limited to a few large players, which leads to market fragmentation and a lack of competition and ultimately inhibits innovation.[53] Against this backdrop, the **Data Act**[54] (German: Datenverordnung), which came into force on 11 January 2024, represents a legislative move aimed at facilitating access to and use of data and moving closer to the goal of a **single European market for data** as proclaimed in the **European data strategy**[55] - Europe should take a leading position in the global data economy.[56] The Data Act is the world's first horizontal legal framework for the cross-sectoral access, exchange and use of data, and it is complementary to the Data Governance Act[57] (DGA), which came into force in 2022.[58]

Specifically, the Data Act establishes binding EU-wide rights for data owners, users and third parties that guarantee access to and use of the data generated by smart products. At the same time, the Data Act contains provisions to prevent disproportionate contractual conditions and the misuse of data access rights, as well as measures for switching between cloud providers and promoting the interoperability of data and connected products. In order to improve the management of social emergencies and exceptional situations, the Data Act also includes provisions for facilitating access to data by public authorities.

2. Scope and definitions, Art. 1–2 DA

The scope of the Data Act is largely determined by the provisions of the first chapter: While Art. 1(1)–(3) DA positively describes the territorial, material and personal scope , Art. 2 No. 1–43 DA establishes legal definitions for the undefined legal terms used in the regulation. Finally, Art. 1(5)–(9) DA clarifies

52 McKinsey & Company, The Internet of Things, 2021, p. 9.
53 COM(2022) 68 final, p. 1.
54 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, OJ L, 2023/2854 of 22.12.2023, p. 1–71.
55 Rec. 4 Regulation (EU) 2023/2854; European Commission, Impact Assessment Report Data Act, p. 24.
56 Schreiber K./Pommerening P./Schoel P., Der neue DA, § 3 para. 2.
57 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, pp. 1–44.
58 Hartl K./Vogel P., *LTZ* 2024 (104); for the DGA see II.

that the legal acts and voluntary agreements on data exchange between private and public bodies (6) listed therein remain unaffected by the Data Act. In the event of a conflict between the Data Act and the General Data Protection Regulation[59] (GDPR), the latter takes precedence, Art. 1(5) DA.

a) Territorial scope

The territorial scope is determined by the **market place principle** (Art. 1(3) (a)–f) DA). The connecting factor is therefore the activity within the Union described in Art. 1(3) DA, irrespective of the registered office of the natural or legal person.[60] The establishment of the legal person is therefore not relevant.[61] The only decisive factor is the **placing on the market of** a connected product by the manufacturer or the offering of related services in the Union, i.e. the first making available of a connected product on the Union market (Art. 2 No. 22 DA). The time of first making available is likely to be a **factual consideration**, so that only the actual making available of a specific product type or product series on the Union market is relevant and not the time of the conclusion of a contract or the fulfilment of a sales contract for a specific connected product.[62]

b) Temporal scope

The provisions of the Data Act apply **from 12 September 2025** in accordance with Art. 50 DA, whereby the obligation to make product data and related service data available to the user in accordance with Art. 3(1) DA only applies to connected products and services related to them placed on the market after 12 September 2026. In addition, the provisions of Chapter 3 (Obligations of data holders) only apply to data provision obligations that come into force after 12 September 2025. Finally, the provisions of Chapter Four (Unfair contractual terms related to data access and use between enterprises) only apply to contracts concluded after 12 September 2025 or, from 12 September 2027, to contracts concluded on or before 12 September 2025, provided that they are concluded for an indefinite period (a) or their term of validity ends no earlier than 10 years after 11 January 2024 (b).

c) Material scope

The material scope of the Data Act is initially determined declaratively by Art. 1(2) DA, according to which the regulation extends to both personal and non-personal data.[63] Art. 1(2) DA then declares chapters two to seven to be applicable to various categories of data:

---

59 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; OJ L 119, 4.5.2016, p. 1–88.

60 Bomhard, D., *MMR* 2024, 71, 72.

61 Schreiber K./Pommerening P./Schoel P., Der neue DA, § 3 para. 14.

62 Schreiber K./Pommerening P./Schoel P., Der neue DA, § 3 para. 27, 33.

63 Critical of the function of the standard Schreiber K./Pommerening P./Schoel P., Der neue DA, § 3 para. 11; Bomhard, D., *MMR* 2024, 71 (72).

- Chapter 2 (BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING) to data, with the exception of content, concerning the performance, use and environment of connected products and related services (a);
- Chapter 3 (OBLIGATIONS FOR DATA HOLDERS OBLIGED TO MAKE DATA AVAILABLE PURSUANT TO UNION LAW) to any private sector data that is subject to statutory data sharing obligations (b);
- Chapter 4 (UNFAIR CONTRACTUAL TERMS RELATED TO DATA ACCESS AND USE BETWEEN ENTERPRISES) to any private sector data accessed and used on the basis of contract between enterprises (c);
- Chapter 5 (MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, THE COMMISSION, THE EUROPEAN CENTRAL BANK AND UNION BODIES ON THE BASIS OF AN EXCEPTIONAL NEED) to any private sector data with a focus on non-personal data (d);
- Chapter 6 (SWITCHING BETWEEN DATA PROCESSING SERVICES) to any data and services processed by providers of data processing services (e);
- Chapter 7 (UNLAWFUL INTERNATIONAL GOVERNMENTAL ACCESS AND TRANSFER OF NON-PERSONAL DATA) to any non-personal data held in the Union by providers of data processing services (f).

The most important definitions that characterise the material scope of the Data Act are presented below.

aa) Data, Art. 2 No. 1 DA

The central concept of **data** is defined in Art. 2 No. 1 DA as

> any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording.

A look at Art. 2 No. 1 DGA and Art. 2 No. 24 DMA shows that the European legislator has opted for a standardised definition of data within the framework of the Digital Rights Act.[64]

(1) Primary data

According to the recitals, **primary data** in particular is covered by the scope of the Data Act.[65] Primary data is data in raw form that relates to data points and is generated automatically without any further form of processing, which is why it is also referred to as **source data** or **raw data**.[66]

(2) Processed data

In addition to primary data, **processed data** is also covered by the definition of data in Art. 2 No. 1 DA.[67] Processed data is data that is contextualised prior to further processing as part of the processing

64 Wiebe, A., *GRUR* 2023, 1569 (1570), has already taken this line.
65 Rec. 15 Regulation (EU) 2023/2854.
66 Rec. 15 Regulation (EU) 2023/2854.
67 Rec. 15 Regulation (EU) 2023/2854.

procedure in order to make it understandable and usable.[68] For example, this could be data from a robotic mower that uses sensors to measure the physical conditions of the environment, such as the temperature or pH value of the ground to be mowed.[69] However, this only applies if the processing of the data is not the result of **significant additional investment**, as is the case with processing using complex proprietary algorithms.[70] Such data often affects the intellectual property rights of the data owner and can also be characterised as **highly processed data** due to the complex processing it undergoes.[71] In practice, such investments are often passed on to the customer and included in the sales price. This raises the question of whether the criterion of significant additional investment requires the data owner to incur ongoing costs for the data preparation process or whether one-off costs in the development process are sufficient, even if the costs are borne indirectly by the customer.

Although the clarification provided by the Commission in the FAQ[72] helps to clarify the concept of data, difficult questions of demarcation are likely to continue to arise in practice, as the following examples illustrate.[73] For example, the temperature of a connected product is likely to be indisputably regarded as primary data. However, it is difficult to categorise the result of a temperature error message that occurs, as a comparison between the target and actual temperature takes place in a separate step. The target temperature may even be calculated with the aid of complex algorithms from data from other sensors (e.g. altitude above sea level, humidity, air pressure), meaning that the data from the connected product could be primary data (temperature) and processed or highly processed data (the result of the error message). In practice, the decisive factor will therefore be when the criterion of significant additional investment is fulfilled.

Delimitation difficulties also arise when **the data is processed within a** connected **product**: For example, the longitude and latitude of a GPS datum must be categorised as primary data. However, the specific address can be determined using proprietary software in the connected product. This again raises the question of whether the determination of the address is processed data or whether the software, viewed in isolation, represents a related service, which would qualify the address as related service data. From this perspective, however, it is not necessary to distinguish between processed data and primary data. More helpful than the investment criterion in such cases could be the differentiation according to whether the processing of the data takes place inside or outside the connected product.

Furthermore, the demarcation criterion of significant investment is unlikely to provide any relief in many cases, as the preparation process may be complex but is based on the design of the product and does not always require a high level of investment. In a connected product, for example, there may be numerous

---

68 European Commission, FAQ DA, p. 6; Niehaus, M./Siems, J., *ZdiW* 2024, 50 (53).
69 Rec. 15 Regulation (EU) 2023/2854.
70 Rec. 15 Regulation (EU) 2023/2854; Kim, D., *MMR* 2024, 87 (89).
71 European Commission, FAQ DA, p. 7.
72 https://digital-strategy.ec.europa.eu/de/library/commission-publishes-frequently-asked-questions-about-data-act.
73 Wiedemann, N./Conrad, T./Salemi, S., *K&R* 2024, 157 (161).

sensors that measure the effects on the product. The manufacturer of such a product has divided the sensors into groups (zones) in order to be able to better describe the localisation of the impact on the product. It is difficult to classify the data filtered by the zone categorisation as processed data, as the product only passes on aggregated information about the affected zones and not the detailed sensor information to the backend. Whether this filtering is considered sufficient processing to speak of highly processed data remains questionable, as there is no complex and cost-intensive processing in the narrower sense. In cases where data is merely filtered or aggregated within the product, it is therefore more likely to be derived data or even primary data that is covered by the data concept of Art. 2 No. 1 DA.

(3) Metadata, Art. 2 No. 2 DA

Unlike processed data, metadata serves to give other data a certain context[74] and to enable structured use of this data.[75] It is a structured description of the content or use of data that makes it easier to find or use that data (Art. 2 No. 2 DA). Metadata can have a positive impact on innovation and the development of digital services, for example by being used for the maintenance and repair of connected products.[76] For this reason, the basic context and, where applicable, timestamps of the metadata should also be recorded.[77] If metadata is collected in connection with the data brokerage services offered, it may only be used for selected purposes, such as the further development of the service or to promote information security.[78] The definition of data in Art. 2 No. 2 DA of the DA does not include metadata that is generated during the creation of text, audio or audiovisual content.[79]

Metadata must be distinguished from data resulting from additional expenditure (derived data); such data are excluded from the scope of the DA.[80]

(4) Product data, Art. 2 No. 15 DA

Another important category of data is that of product data. Art. 2 No. 15 DA defines this as data generated by the use of a connected product and designed by the manufacturer to be accessible via an electronic communication service, physical connection or on-device access by a user, data holder or third party, including, where applicable, the manufacturer. This includes not only data generated during active use, but also data generated while the user is inactive.[81] However, data that is purely descriptive of the product does not fall under product data according to Art. 2 No. 15 DA.[82] The DA itself does not give

74 Niehaus, M./Siems, J., *ZdiW* 2024, 50 (53).
75 Schreiber K./Pommerening P./Schoel P., Der neue DA, § 4 para. 53.
76 Rec. 15 Regulation (EU) 2023/2854.
77 Rec. 15 Regulation (EU) 2023/2854.
78 Schreiber K./Pommerening P./Schoel P., Der neue DA, § 12 para. 99.
79 Heinzke, P./Herbers, B./Kraus, M., *BB* 2024, 649 (650); Rec. 16 Regulation (EU) 2023/2854.
80 Schild, H.H., 'DA Art. 2', in: BeckOK Datenschutzrecht, para. 20.
81 Wentzel, C./Lutz, B., *RAW* 2024, 123, 126; Rec. 15 Regulation (EU) 2023/2854.
82 European Commission, FAQ DA, p. 6.

rise to any claims that certain data can be collected; such a claim can only arise from sector-specific regulation.[83]

(5) Related service data, Art. 2 No. 16 DA

In addition, the DA also applies to related service data, i.e. data that represents the digitisation of user actions or processes in connection with the connected product and is intentionally recorded by the user or generated as a by-product of the user's action during the provision of a related service by the provider (Art. 2 No. 16 DA). Whether the data is generated intentionally or accidentally by the user's actions is irrelevant for the application of the DA.[84] For related service data, however, it is important that they are generated by the user in the networked use.[85] Data that is generated in connection with a related service, but which cannot itself be attributed to the actual product, is not subject to the Data Act. This includes, for example, repair or maintenance services.[86]

(6) Readily available data, Art. 2 No. 17 DA

Furthermore, readily available data is also addressed. This is product data and related service data that a data holder lawfully obtains or can obtain from the connected product or related service without disproportionate effort, going beyond simple processing (Art. 2 No. 17 DA). However, there are no further indications in the Data Act as to when data is readily available.[87] It is only clear that data generated during product use is exempt, unless the product is designed to store or transmit such data.[88] In this respect, however, an economic approach is appropriate, which involves comparing the economic cost of making the data available with the value of the consideration.[89] If the economic cost is low, the date is one that is readily available.

(7) Data generated by virtual assistants, Art. 1(4) DA

Finally, the data generated by virtual assistants is also partially covered by the scope of the Data Act. This is based on the legal provision of Art. 1(4) DA, according to which the rules for connected products or related services also apply to virtual assistants if they interact with a connected product or related service. In this respect, the data collected by the virtual assistant from the relationship between the user and the related service or connected product is also covered by the scope of the Data Act.[90] This is also the case if the virtual assistant service used is neither a connected product nor a related service.[91]

---

83 Niehaus, M./Siems, J., *ZdiW* 2024, 50, 52.
84 Schreiber K./Pommerening P./Schoel P., Der neue DA, § 4 para. 39.
85 Schild, H.H., 'DA Art. 2', in: BeckOK Datenschutzrecht, para. 92.
86 Niehaus, M./Siems, J., *ZdiW* 2024, 50 (52).
87 Wiedemann, N./Conrad, T./Salemi, S., *K&R* 2024, 157 (161).
88 Rec. 20 Regulation (EU) 2023/2854.
89 Niehaus, M./Siems, J., *ZdiW* 2024, 50 (53).
90 Niehaus, M./Siems, J., *ZdiW* 2024, 50 (54).
91 Schreiber K./Pommerening P./Schoel P., Der neue DA, § 4 para. 43.

(8) Data and content not recorded

A synopsis of Art. 1(2) (a) DA and recital 16 shows that **content**, i.e. text, audio or visual representations, are not covered, which requires separate clarification in light of the very vague definition.[92] Content generated by connected products such as smartphones, tablets or computers, as well as the metadata created when the content is generated, are therefore not data within the meaning of Art. 2 No. 1 DA.[93] Nevertheless, difficult questions of demarcation also arise here, especially when connected products consist of many components. For example, almost every smartphone contains a camera. A camera only captures light signals and converts them electrically into an overall image. This raises the question of whether the images from the camera installed in a connected product are to be regarded as derived data or as content within the meaning of recital 16. The fact that the brightness of the individual pixels represents primary data, from which the overall image is derived, speaks in favour of classification as derived data. On the other hand, the fact that the customer has purchased a connected product (smartphone) with a camera and therefore expects a camera image speaks in favour of classifying the overall image as content. The decisive factor for the question of whether it is content or derived data is therefore likely to be the perspective to be adopted for the legal assessment.

As shown above, **information derived** from processed data also does not fall within the scope of the Regulation, according to recital 15.[94] This applies in particular to information obtained from the processing of data using complex algorithms, as this is (possibly) information protected by intellectual property rights. Examples include information obtained by means of sensor data fusion[95].[96]

In summary, primary data, processed data, metadata, product data, related service data, readily available data and data generated by virtual assistants are covered by the scope of the Data Act, but not content and derived data.[97]

bb) Connected product, Art. 2 No. 5 DA

Another central concept of the Data Act is that of the connected product. According to Art. 2 No. 5 DA, a **connected product** is an object that obtains, generates or collects data about its use or environment and that can transmit product data via an electronic communications service, physical connection or on-device access and whose primary function is not the storage, processing or transmission of data on behalf of any party other than the user.

The term "connected product" is concretised by recital 14, according to which connected products obtain, generate or collect data by means of their components or operating systems. In particular, terrestrial

92 Heinzke, P./Herbers, B./Kraus, M., *BB* 2024, 649.
93 Heinzke, P./Herbers, B./Kraus, M., *BB* 2024, 649.
94 Critical of this is Kerber, W., GRUR Int 2023, 120 (127); for more details see A.I.2.c).aa).(2).
95 Sensor data fusion is a process in which data from multiple sensors is combined to obtain a more accurate and comprehensive picture of a situation or object than with a single sensor, *Alpaydin*, Machine Learning, p. 553.
96 Rec.15 Regulation (EU) 2023/2854.
97 Niehaus, M./Siems, J., *ZdiW* 2024, 50 (52).

telephone networks, cable television networks, satellite networks and near-field communication networks are cited as examples of electronic communication services.[98] In practice, this will regularly involve **Internet of Things (IoT)** products such as smartphones, smart home devices, wearables, networked household appliances, smart TVs or modern manufacturing machines that are networked in production processes in order to exchange operating data.[99] Data from prototypes, on the other hand, is excluded.[100] However, the Data Act only covers connected products that have been placed on the Union market in accordance with Art. 2 No. 22 DA. Placing on the market always refers only to an individual product and never to all products of this type or the entire product category.[101]

cc) Related service, Art. 2 No. 6 DA

A *related service* is defined in Art. 2 No. 6 DA as a digital service, other than an electronic communications service, including software, which is connected to the product at the time of purchase, rental or lease in such a way that the connected product could not perform one or more of its functions without it, or which is subsequently connected to the product by the manufacturer or a third party in order to supplement, update or customise the functions of the connected product.

Related services are therefore usually a functional addition to the connected product, which are either already integrated when the product is purchased or can be added later as an option.[102] Neither the contractual typological assessment of the service nor by whom the service is provided is relevant for the classification as a related service. It is therefore not decisive whether the service is provided by the provider of the connected product or by an independent third party.[103] The decisive factor for the legal assessment is that the related service transmits data or commands to the connected product that have an influence on the functions, behaviour or operation of the product.[104] It is necessary that the data exchange between the connected product and the provider is bilateral.[105] One such command from the related service would be the transmission of a software update to the connected product. Cloud-based services, which are necessary to fully utilise the functions of smart products such as networked household appliances, vehicles or consumer electronics, are also a practical example.

The courts will have a crucial role to play in determining the function of a connected product, in particular in distinguishing between a digital service and a related service.[106] There is no related service within the meaning of the standard if the service does not have a direct impact on the operation or function of the product and if no data or commands are transmitted to the product.[107] Recital 17 gives the examples

98 Rec. 15 Regulation (EU) 2023/2854.
99 European Commission, FAQ DA, p. 8; Sebulke, P./Ehlen T., *CR* 2024, 84 (85).
100 Rec. 14 Regulation (EU) 2023/2854.
101 European Commission, FAQ DA, p. 8.
102 European Commission, FAQ DA, p. 9; Apel, S./Huber, C., *JuS* 2024, 410 (412).
103 Rec. 17 Regulation (EU) 2023/2854.
104 European Commission, FAQ DA, p. 9; Rec. 17 Regulation (EU) 2023/2854.
105 European Commission, FAQ DA, p. 9.
106 European Commission, FAQ DA, p. 9.
107 Rec. 17 Regulation (EU) 2023/2854.

of consultancy services, analyses, financial services or maintenance services - such services are not directly related to the functions of the connected product. Basic infrastructure services such as power supply or the provision of an internet connection are also expressly not a related service within the meaning of Art. 2 No. 6 DA.[108]

In summary, related services are usually services provided by the provider of connected products or an independent third party that are closely functionally related to the operation of a connected product, enabling or extending its functions by transmitting data or commands that influence the behaviour of the product.

dd) Virtual assistants, Art. 2 No. 31 DA

The DA not only covers connected products and related services, but also extends to so-called **virtual assistants**, insofar as they interact with the connected product or related service (Art. 1(4) DA).

According to the legal definition in Art. 2 No. 31 DA, this is software that can process orders, tasks or questions, including on the basis of input in audio and written form, with gestures or movements, and that grants access to other services or controls the functions of connected products on the basis of these orders, tasks or questions.

By including virtual assistants in the scope of the Data Act, the legislator is recognising the increasing importance of services such as '*Apple's Siri', 'Google Assistant'* and '*Amazon's Alexa',* which are becoming more and more important in people's everyday digital lives. They often act as a means of communication between people and the connected products and related services they use.[109] Based on the data collected, they can provide information about how people use smart products and interact with them.[110] This is explicitly not intended to apply to data that is collected by the virtual assistant but is not related to the connected product or service.[111]

However, it is unclear to what extent virtual assistants can be distinguished from related services, as overlaps are conceivable in this respect.[112]

ee) Data processing service, Art. 2 No. 8 DA

A **data processing service** is a digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction (Art. 2 No. 8 DA).

---

108 Rec. 17 Regulation (EU) 2023/2854.
109 Rec. 17 Regulation (EU) 2023/2854.
110 Rec. 17 Regulation (EU) 2023/2854.
111 Rec. 17 Regulation (EU) 2023/2854.
112 Bomhard, D., *MMR* 2024, 71 (73).

Data processing services are therefore generally characterised by the fact that they store, process or analyse (large) amounts of data on behalf of the user and make it available to the user on demand.[113] The term data processing service therefore includes providers of cloud services such as *'Amazon Web Services' (AWS)* or web analytics services such as *'Google Analytics'*.[114]

Network access, which is made possible via the data processing services, should be location-independent, i.e. via web browsers and mobile devices as well as workstation computers.[115]

In simple terms, switching refers to a process in which a customer switches from one data processing service to another service of the same or a similar type. This process may occur either between different providers of data processing services or to an in-house ICT infrastructure and involves the extraction, conversion and transfer of data.

d) Personal scope

The personal scope is determined by the triangular relationship defined by the Data Act, consisting of the user, the data holder and the data recipient.[116]

aa) User, Art. 2 No. 12 DA

According to Art. 2 No. 12 DA, a **user** is a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services.

In accordance with the legislative concept, the user under Art. 2 No. 12 DA will therefore regularly be the purchaser and owner of the connected product[117]. However, it should be noted that tenants or lessees can also be considered users.[118] With regard to related services, the user is defined as the individual who utilises the related service.[119] In addition to consumers as natural persons, companies in the sense of legal entities and public bodies can also be considered users.[120]

The DA is intended to ensure that the user has timely access to the data that has been generated by their utilisation of the connected product or related service.[121] In addition to the utilization of data, the user may also elect to make it available to third parties of their choosing.[122] This is based on the idea that the

113 Rec. 80 Regulation (EU) 2023/2854.
114 Rec. 81 Regulation (EU) 2023/2854.
115 Rec. 81 Regulation (EU) 2023/2854.
116 See also the illustration under 4 Rights and obligations.
117 Hoeren, T., *MMR* 2023, 32 (33); also Specht-Riemenschneider, L., *MMR* 2022, 809 (814), according to which only the authorised possession is important.
118 See Schmidt-Kessel, M., *MMR* 2024, 75 (77); Schild, H.H., 'DA Art. 2', in: BeckOK Datenschutzrecht, para. 12.
119 Schreiber K./Pommerening P./Schoel P., Der neue DA, § 4 para. 21.
120 Rec. 18 Regulation (EU) 2023/2854.
121 Rec. 5 Regulation (EU) 2023/2854.
122 Rec. 5, 35 Regulation (EU) 2023/2854.

user benefits from the advantages of use, but also bears the risks of use and as such should be entitled to a right of access.[123]

Art. 2 No. 12 DA is linked both to the legal situation in rem (owns)[124] and alternatively (or)[125] to the causal transaction underlying the use ("to whom temporary rights to use that connected product have been contractually transferred"). Recital 18 appears to contradict this, according to which it is not the contractually granted use of the connected product that is important, but rather temporary rights of access to data from the connected product.[126] This concretisation of the concept of user is not convincing for the following reason: The primary regulatory objective of the Data Act is to strengthen the position of users of connected products, as data is only generated through their digital user actions.[127] Nevertheless, the granting of temporary access rights to data can occur without the involvement of the user, thereby rendering the user's actual and contractual rights to the connected product irrelevant for the determination of the user within the meaning of Art. 2 No. 12 DA. Such a consideration would rather weaken the position of the (actual) user than strengthen it.

By linking both the real and the contractual position of the user to the connected product, the legislator opens up the possibility that there may be several users of a connected product, for example as a result of co-ownership or other contractual agreements.[128] For such connected products, manufacturers should set up mechanisms that allow either the use of one account by multiple individuals or the creation of multiple user accounts.[129] It is evident that the Data Act acknowledges the fact that, in specific scenarios, multiple individuals are involved in the generation of data. A prime example of this is car sharing, wherein the data is generated by the car manufacturer, the car sharing provider, and the user.[130]

Access to the product data or related service data should only be granted to the user upon explicit request.[131] This can be implemented by means of a request procedure.[132]

The sphere of the user also includes the data subject within the meaning of Art. 4 No. 1 GDPR. It may or may not be the same person as the user.[133] If the user and the data subject are different, the user

123 Rec. 18 Regulation (EU) 2023/2854; Schreiber K./Pommerening P./Schoel P., Der neue DA, § 4 para. 21.
124 This is an incorrect translation of the English term "owns", Antoine, L., *CR* 2024, 1 (3) (fn. 40).
125 A. A. Sprecht-Riemenschneider, L., MMR 2022, 809 (813) et seq.
126 Antoine, L., *CR* 2024, 1 (3).
127 Rec. 6 Regulation (EU) 2023/2854.
128 This is also expressly stated in Rec. 18, 21 Regulation (EU) 2023/2854; Schreiber K./Pommerening P./Schoel P., Der neue DA, § 4 para. 21; Dannhausen, E./Abel, D., *MMR* 2024, 931; McGuire, R./Schulte-Nölke, H., *ZdiW* 2024, 73, 75; Antoine, L. CR 2024, 1, 4, is dismissive with regard to relationships of convenience.
129 Rec. 21 Regulation (EU) 2023/2854.
130 Rec. 18 Regulation (EU) 2023/2854; on the associated legal complexity Antoine, L., CR 2024, 1 (4).
131 Rec. 21, 35 Regulation (EU) 2023/2854.
132 Rec. 21 Regulation (EU) 2023/2854.
133 Rec. 7 Regulation (EU) 2023/2854; Steinrötter, B., *GRUR* 2023, 216 (220).

assumes the role of controller in accordance with Art. 4 No. 7 GDPR.[134] This is because the assertion of the right of access by the user results in data processing in accordance with Art. 4 No. 2 GDPR.[135]

bb) Data holder, Art. 2 No. 13 DA

Data holder is defined in Art. 2 No. 13 DA as a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service.

In contrast to the English version of the *Data Holder*, the legal definition of the data holder according to the German translation of the Data Act can - as has already been criticised in the literature - give the impression that it is only about data that was retrieved or generated during the provision of a related service, which means that product data from connected products falls outside the scope.[136] Furthermore, it is criticised that, according to the German definition, product and related service data incorrectly only appear to be relevant in the context of a contractual agreement.[137] Therefore, according to the English wording, a data holder under Art. 2 No. 13 DA is a person who has the right or obligation to use and provide data, including - if contractually agreed - product data or related service data that they have retrieved or generated during the provision of a related service.[138]

The definition of data holder has also been heavily criticised elsewhere for its lack of precision and circularity:[139] For example, an authorisation or obligation is assumed under applicable Union law, but this is only determined by the DA.[140] In order to determine the data holder, it will therefore be necessary to look at who has **de facto control** over the data.[141] Although it does not matter who manufactured the software or hardware[142], in practice, the manufacturer of the connected product will regularly be the data holder, as it has control over the technical design of the product.[143] Control over the technical design was a feature of the data holder that was still provided for in the Commission's draft DA, but this does not necessarily mean that this is a deliberate departure from de facto control as a limiting feature.[144] However, without a de facto possibility of access, the categorisation as data holder is unlikely, as a possibility of control by the data holder is implicitly assumed in Art. 4(1) and Art. 5 (1) DA.[145] In this

134 Schreiber, K./Pommerening, P./Schoel, P., Der neue DA, § 4 para. 22.
135 Schreiber, K./Pommerening, P./Schoel, P., Der neue DA, § 4 para. 22.
136 Instead of all of them, see Wiedemann, N./Conrad, T./Salemi, S., *K&R* 2024, 157 (160).
137 Wiedemann, N./Conrad, T./Salemi, S., *K&R* 2024, 157 (160).
138 Wiedemann, N./Conrad, T./Salemi, S., *K&R* 2024, 157 (160).
139 Heinzke, P./Herbers, B./Kraus, M., *BB* 2024, 649; Bomhard, D./Merkle, M., *RDi* 2022, 168 (169); Wiedemann, N./Conrad, T./Salemi, S., *K&R* 2024, 157 (159); Statement of the German Bar Association, 2022, p. 12 et seq.
140 Keppeler, L./Schneider, R./Nickel, A. *ITRB* 2024, 180 (181).
141 Hartl, K./Vogel, P., *LTZ* 2024, 104 (105).
142 European Commission, FAQ DA, p. 15.
143 McGuire, R./Schulte-Nölke, H., *ZdiW* 2024, 73 (75).
144 Schmidt-Kessel, M., *MMR* 2024, 75 (77).
145 European Commission, FAQ DA, p.16; Antoine, L. *CR* 2024, 1 (4); Schmidt-Kessel, M., *MMR* 2024, 75 (77); Heinzke, P./Herbers, B./Kraus, M., *BB* 2024, 649.

context, the question of the extent to which technical obstacles to performance affect categorisation as data holder is also raised.[146]

However, it is also conceivable that a company that offers a service associated with a connected product, i.e. an related service, is the data holder.[147]

cc) Data recipients and third parties, Art. 2 No. 14 DA

According to the legal definition of Art. 2 No. 14 DA, a data recipient is a natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law. In contrast to the user and the data holder, data recipients therefore have no relationship to the connected product or the related service.[148] According to the definition, data recipients cannot be consumers, as a commercial, business, craft or professional activity is always assumed.[149]

As indicated by the wording, the DA stipulates a distinction between the data holder and the data recipient, who, by definition, should not be the same individual. Instead, the legislation outlines the requirement for a relationship to be established between these two parties.[150] Art. 8 DA deals in more detail with the conditions under which data holders provide data to data recipients. The data recipient is therefore the party who receives data from a data holder at the request of the user.[151] Since a data holder retrieves or generates *its* own data in accordance with Art. 2 No. 13 DA by virtue of de facto control[152] - and thus *controls* it in this respect - it cannot therefore receive this data in accordance with Art. 2 No. 14 DA. Within the context of a single legal relationship, it is therefore not possible for a data holder to concurrently serve as a data recipient.[153] The situation is only different if a data holder is provided with other data by another data holder at the request of a user: Then the legal nature of the data holder ceases to apply to this relationship and he becomes the data recipient, Art. 2 No. 14 DA.

At the request of the user, certain data may be provided to a **third party**.[154] In this particular instance, the third party is considered to be the data recipient, as outlined in Art. 2 No. 14 DA.[155] The term data recipient also includes third parties to whom data is provided in accordance with a legal obligation under

146 Rejecting Schmidt-Kessel, M., *MMR* 2024, 75 (77); Heinzke, P./Herbers, B./Kraus, M., *BB* 2024, 649 (650).
147 European Commission, FAQ DA, p. 15.
148 Kraft, T./Schumann, S., *GRUR Prax* 2024, 324 (325).
149 Kraft, T./Schumann, S., *GRUR Prax* 2024, 324 (325).
150 See Art. 1(1)(b) DA: "This Regulation contains harmonising rules, inter alia, on the provision of data by data controllers to data recipients."
151 Schild, H.H., 'DA Art. 2', in: BeckOK Datenschutzrecht, para. 86.
152 See d.) bb) "Data controller, Art. 2 No. 13 DA".
153 In conclusion also Schreiber, K./Pommerening, P./Schoel, P., Der neue DA, § 4(13)–(23).
154 Art. 5(1) DA.
155 Schreiber, K./Pommerening, P./Schoel, P., Der neue DA, § 4(23).

other Union law or under national legislation adopted in accordance with Union law (Art. 2 No. 14 DA).[156]

dd) Manufacturer

The term "*manufacturer*" is not legally defined, but is assumed in various regulations.[157] However, the recitals offer some insights into this matter, stating that the manufacturer exercises control over the design and development of the connected product or related service and therefore plays a pivotal role in the generation of IoT data.[158] Based on the recitals, the manufacturer is therefore the legal or natural person who develops and designs a connected product and can influence the design of the product by virtue of factual or legal relationships.[159]

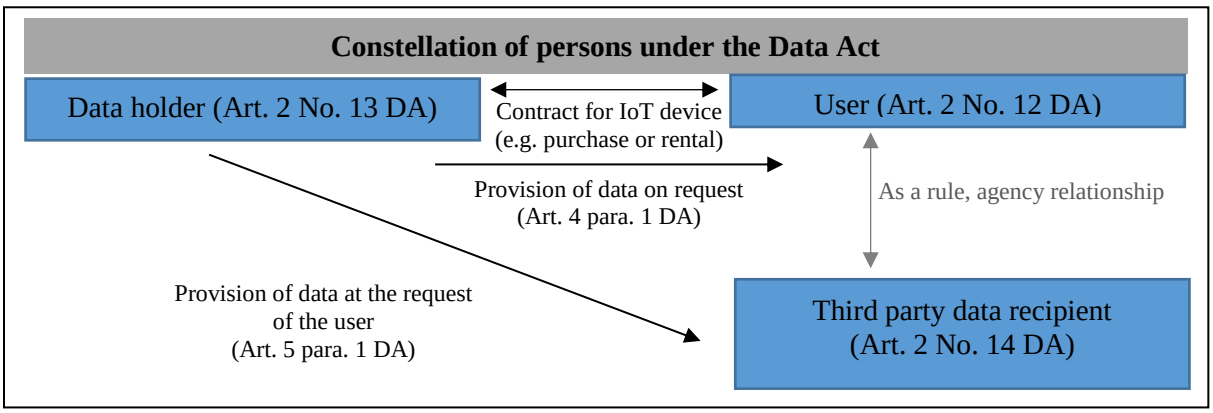
ee) Contractual partner of the user

Contractual partners of the user play a comparatively subordinate role in the personal structure of the Data Act. They may be the seller, lessor or lessee of a connected product or a related service. According to the wording of Art. 3(2) DA, the legislator assumes that the contractual partner and the manufacturer can be identical. Only the legal relationship with the user is likely to be decisive for determining the user's contractual partner.[160] The information obligations of Art. 3(2), (3) DA apply to them.

3. Rights and obligations of data holders, users and data recipients

a) Introduction

The core of the Data Act consists of the rights and obligations of the parties involved with regard to the access, use and transfer of data (Chapters II, III, IV, X DA). The relationships between data holders, users and data recipients can be summarised as follows:[161]



156 Schreiber, K./Pommerening, P./Schoel, P., Der neue DA, § 4 para. 23.
157 For example Art. 1(3)(a) DA or Art. 3(1) DA.
158 Rec. 6, 14, 15, 20, 21 Regulation (EU) 2023/2854.
159 Schreiber, K./Pommerening, P./Schoel, P., Der neue DA, § 4 para. 15 refer to this as a result-orientated interpretation.
160 Schreiber, K./Pommerening, P./Schoel, P., Der neue DA, § 4 para. 20.
161 The diagram is taken from Hoeren, T./Pinelli, S., IT Contract Law, p. 413.

All of these persons can - and are authorised to - use, request or pass on the data concerned in accordance with the requirements of the Data Act. The following description attempts to illustrate their rights and obligations to the data concerned and between each other in accordance with the underlying concept of the Data Act: Firstly, the data holder has *de* facto *control*[162] over the data generated[163] . They are also at liberty to utilise the data, provided that a contract is in place with the user.[164] In contrast, the user possesses comprehensive authorisation to utilise the data.[165] However, in order to access the data, they must be granted access by the data holder. At the request of the user, data recipients can also be granted access to the data in question. If a dispute arises over the individual legal relationships, the Data Act provides for dispute resolution procedures before so-called dispute resolution bodies.

b) Obligations of the data holder when using the data

The principal objective of the Data Act is to grant the user of a connected product or related service greater autonomy in the management of data generated through its utilisation.[166] The starting point is initially the ***de* facto *control*** of the data holder over the generated data.[167] This corresponds to previous industry practice, as manufacturers can freely dispose of all generated data through design decisions.[168] The legislator did not aim to exclude the control of the data holder by granting the user absolute rights of access and use.[169] In this respect, a decision was made at the executive level against recognising so-called **data ownership**[170].[171] Instead, the user is granted access to the data alongside the data holder, either through direct access (so-called *accessibility-by-design,* Art. 3(1) DA*)* or through access on request (Art. 4(1) DA). The Data Act does not stand in the way of the data holder's technical data sovereignty.[172] Some even have interpreted the regulation as an endorsement.[173]

It is imperative to establish the extent to which the data controller may utilise the data, and the purpose for which this utilisation is intended. In principle, the data holder may only use available, non-personal data without further ado on the basis of a contract with the user in accordance with Art. 4(13) DA. The data may only be made available to third parties in accordance with Art. 4(14) DA for the fulfilment of

---

162 Rec. 5 Regulation (EU) 2023/2854; Antoine, L., *CR* 2024, 1 (2); Keppeler, L./Schneider, R./Nickel, A., *ITRB* 2024, 180 (183); Kerber, W., *JoAE* 2024, 1 (2) et seq.; Specht-Riemenschneider, L., *MMR* 2022, 809 (815).

163 See bullet point 2 c) aa).

164 This follows for non-personal data from Art. 4(13) DA. For personal data, all justification grounds under Art. 4(12) DA in conjunction with Art. 6, 9 GDPR come into consideration; see Raue, B., 'DA Art. 4', in: BeckOK Datenschutzrecht, para. 76.

165 Rec. 30 Regulation (EU) 2023/2854.

166 Rec. 5 Regulation (EU) 2023/2854; Kerber, W., *GRUR Int.* 2023, 120 (122).

167 Rec. 5, 20 Regulation (EU) 2023/2854; Antoine, L *CR* 2024, 1 (2); Keppeler, L./Schneider, R./Nickel, A, *ITRB* 2024, 180 (183); Kerber, W., *JoAE* 2024, 1 (2) et seq.; Podszun, R./Pfeifer, C., *GRUR* 2022, 953 (956); Specht-Riemenschneider, L., *MMR* 2022, 809 (815).

168 Kerber, W., *JoAE* 2024, 1 (2) et seq.

169 Rec. 6 Regulation (EU) 2023/2854; on the inconsistent wording of Art. 4(13) DA (Art. 4(6) COM(2022) 68 final) Drexl, J., et al, Data Act, para. 44–55.

170 In detail on data ownership Hoeren, T., in Pertot, T. (ed.), Rechte an Daten, 2020, p. 37 et seqq.

171 In agreement with Specht-Riemenschneider, L., *MMR* 2022, 809 (818).

172 Kerber, W., *GRUR Int.* 2023, 120 (130) et seq.; Specht-Riemenschneider, L., *MMR* 2022, 809 (815).

173 Kerber, W., *GRUR Int.* 2023, 120 (128); Specht-Riemenschneider, L. *MMR* 2022, 809 (818).

the contract with the user. The data holder may contractually prohibit third parties from re-disclosing the data, Art. 4(14) DA. In addition to the Data Act (Art. 1(5) DA, the requirements of Art. 6(1) GDPR apply to personal data due to the application of the GDPR.

In the following, the use of the data by the data holder will be analysed in more detail on the basis of practical questions. *De facto*, the data holder has control over the data. However, a user agreement pursuant to Art. 4(13) DA is required for its use (see 3.b)aa)); the deletion of the data can also be categorised as use in the broadest sense.[174] Whether the data holder is authorised to delete data or obliged to store data without an express agreement must also be discussed (see 3.b)bb)). Finally, the question arises as to which technical protective measures data holders can take (Art. 11 DA) in order to protect their own use of the data and their other interests (see 3.b)cc)).

aa) Usage agreement requirement for readily available data (Art. 4(13) DA)

According to Art. 4(13) DA, the usage agreement requirement only applies to **readily available data**. According to Art. 2 No. 17 DA, this refers to data that a data holder lawfully obtains or can obtain from the connected product or related service without disproportionate effort. Data that is not stored or transmitted outside of the components generating it or the product as a whole is not intended by the legislator to be readily available data.[175] Any other categorisation would appear to be inappropriate anyway, at least with regard to the usage agreement requirement under Art. 4(13) DA, as the data holder cannot use data that they cannot retrieve from the device.

The criterion of "without disproportionate effort" is unlikely to be of particular importance in the context of Art. 4(13) DA; rather, it is unclear why the data holder should be allowed to use data that is difficult to obtain without a user agreement. This feature is more likely to be relevant for the data disclosure request pursuant to Art. 4(1) DA.[176] As a result, according to the view expressed here, the use of all generated, accessible (non-personal) data by the data holder requires the consent of the user in the form of a contract.[177]

(1) Buy-out contracts

Cases are conceivable in which the data holder only provides the connected product or only grants the user use of the service if the user in turn authorises full use of the data within the meaning of Art. 4 (13) DA (so-called **buy-out contracts**).[178] The situation is exacerbated if this contract extends to the sale of the generated data.[179]

---

174 Cf. on erasure as processing in the sense of data protection law Schild, H., ‘GDPR Art. 4(53) et seq.
175 Rec. 20 Regulation (EU) 2023/2854.
176 See 3 b) bb).
177 Antoine, L., *CR* 2024, 1 (2).
178 Specht-Riemenschneider, L., *MMR* 2022, 80 (817).
179 See Kerber, W., *GRUR Int.* 2023, 120 (132).

The Commission's draft was criticised for not adequately addressing the problem of *buy-out contracts*.[180] According to the Commission's draft, the data holder would be free to unilaterally impose such contracts.[181] Corresponding measures were not included in the final version of the Data Act. This means that, for example, sales contracts for connected products that are linked to comprehensively granted rights of use and sale are legally permissible under current law.[182]

(2) Statement

Buy-out contracts appear to be an obstacle to far-reaching protection of user interests, particularly in the B2C business.[183] Originally, the Commission identified "fairness in the digital environment"[184] and consumer participation rights as objectives.[185] Recital 5 DA also speaks of "[preventing] the exploitation of contractual imbalances that hinder fair access to and use of data". Recital 1 DA, however, indicates an intention to promote sustainable economic growth through more data utilisation in general. With the Data Act, the Commission wanted to keep investments in the development of connected products attractive.[186] The Data Act is to be understood as a strongly commercially motivated regulation.[187] While *buy-out contracts* are likely to be difficult to reconcile with the prohibition of discrimination in Art. 7(2) DA, because they disadvantage the user by depriving him of the opportunity to negotiate the rights to the data generated by him under better conditions, they promote the economically lucrative use of data by the data holder.[188] The Data Act therefore falls short of its expectations with regard to the specifically formulated goal of "fairness in the digital environment"[189], at least in the B2C sector.

In business transactions, on the other hand, there is no or at least less informational and behavioural inequality.[190] In some cases, it is even assumed that the product manufacturer is in a weaker position in contract negotiations.[191] In any case, there is no recognisable objective reason to consider *buy-out contracts* in B2B transactions to be inadmissible in contrast to B2C transactions.

---

180 Specht-Riemenschneider, L., *MMR* 2022, 809 (820).
181 Specht-Riemenschneider, L., *MMR* 2022, 809 (817).
182 Translated from Hennemann, M. et al, Data Act, p. 75; Kerber, W., *JoAE* 2024, 1 (4); Steinrötter, B., *GRUR* 2023, 216 (219); Specht-Riemenschneider, L., *MMR* 2022, 809 (809).
183 Kerber, W., *JoAE* 2024, 1 (4).
184 Commission press release of 23 February 2022, https://ec.europa.eu/commission/presscorner/detail/de/ip_22_1113; see European Commission, Impact Assessment Report Data Act, p. 2 et seq.
185 COM(2022) 68 final, p. 3; Assion, S./Willecke, L., *MMR* 2023, 805 (805).
186 European Commission, Impact Assessment Report Data Act, p. 26 et seq.; Kerber, W., *JoAE* 2024, 1 (2).
187 European Commission, Impact Assessment Report Data Act, p. 2 et seq.; Kerber, W., *GRUR Int.* 2023, 120 (127) et seq.; Specht-Riemenschneider, L., *MMR* 2022, 809 (826); see also European Commission, A European Data Strategy, p. 5.
188 The Commission considers the restrictions for manufacturers to be "mitigated" in COM(2022) 68 final, p. 16.
189 Commission press release of 23 February 2022, https://ec.europa.eu/commission/presscorner/detail/de/ip_22_1113; see European Commission, Impact Assessment Report Data Act, p. 2 et seq.
190 Kerber, W., *JoAE* 2024, 1 (4).
191 Kerber, W., *JoAE* 2024, 1 (4).

If one of the contracting parties is a consumer, in particular the user, the current version of the Terms Directive[192] applies (Art. 1(9) DA)[193] and sets limits to the contractual freedom of the data holder. In the B2B context, Art. 13 DA applies.

bb) No authorisation for deletion of the data by the data holder

Deletion of data is a special form of data utilisation in the broadest sense.[194] Whether data holders are authorised to erase data beyond Art. 4(13) DA is not directly apparent from the text of the regulation. The question of an authorisation to erase data is of significant practical relevance, as an absence of such authorisation effectively obliges the storage of data.

In the Commission's draft of the Data Act, the holder of non-personal data was anyone who can provide it to others.[195] This would have allowed the data holder to release themselves from their obligations by deleting the generated data, as the Commission's draft did not provide for an obligation to store the generated data.[196]

The final version of the Data Act defines data holder in Art. 2 No. 13 DA differently than in the draft: the status of data holder is only linked to the legal obligation to provide data. The reasons for the legislator's decision to reorganise the standard remain unclear. However, it is evident that the final legal definition is considerably more compact. This suggests that the objective may have been to enhance the clarity and accessibility of the provision for those who are tasked with the application of the law. On the other hand, entire elements of the offence have been omitted - at least in the wording.

The Data Act does not affect national contract law.[197] If the legislator had intended to amend the regulation not only editorially but also in terms of substantive law through the reorganisation, liability for damages under national contract law[198] would be possible. This would result in the data holder being unable to evade at least secondary liability, which would appear to be in the interests of the data holder, as he is no more worthy of protection in the event of wilful or negligent deletion of the data than the holder of the[199] right to data access that expires as a result. Originally, *Specht-Riemenschneider* had proposed a user's right to data access prior to erasure.[200] However, her underlying criticism of the lack of legal consequences of an unauthorised release of the data holder from liability was addressed by enabling secondary liability.

Overall, it can be assumed that in the final Data Act, the deletion of data by the data holder is not permitted, at least immediately after it has been generated. The wording has now been clarified. The

192 Directives 93/13/EEC, 2005/29/EC and 2011/83/EU in their consolidated version.
193 Schwamberger, S., *MMR* 2024, 96 (98).
194 See Art. 4 No. 2 GDPR.
195 Art. 2 No. 6 COM(2022) 68 final.
196 Rec. 20 Regulation (EU) 2023/2854; Specht-Riemenschneider, L., *MMR* 2022, 809 (820).
197 Rec. 9 Regulation (EU) 2023/2854.
198 In German law according to §§ 280(1), (3), 283 BGB.
199 In German law due to impossibility, § 275(1) BGB.
200 Specht-Riemenschneider, L., *MMR* 2022, 809 (820).

data holder is the party that *generated* the data (Art. 2 No. 13 DA). Moreover, the purpose of user data access would be undermined if the law permitted immediate erasure. In the event of culpable deletion, the data holder is liable.

cc) Technical protective measures, Art. 11 DA

The data holder is entitled to protect itself against unauthorised access to data and violations of Art. 5, 6, 8 and 9 DA by applying suitable **technical protection measures** (Art. 11(1) DA). However, the provision is not intended to extend the far-reaching possibilities of the data holder to protect his interests; rather, it is intended to set limits to them.[201] Of particular relevance in this context is Art. 11(1) DA, which prohibits technical protection measures that treat data recipients differently or restrict the rights of users.[202] A distinction must be made between technical protection measures pursuant to Art. 11(1) DA and technical and organisational measures for the protection of trade secrets (Art. 4(6) DA).[203]

Art. 11(1) DA cites smart contracts[204] and data encryption as examples of permissible protective measures.

If the user violates his obligations under Art. 11(3) DA, the data holder can demand the deletion of the data obtained in this way (Art. 11(3), (2)(a) DA). If the user has gained knowledge from the data and used it to develop a product, the data holder can demand the cessation of the production of the product and the destruction of any stocks (Art. 11(3), (2)(b) DA); the injured party, usually the data holder, must be compensated (Art. 11(3), (2)(d) DA).[205] In contrast, Art. 11(2) DA does not contain any claim for the recall of goods placed on the market or regulations regarding data that has already escaped the access of the unauthorised data recipient. This results from the non-absolute effect of the data holder's rights to the data.[206]

The measures pursuant to Art. 11(2) DA are also available to the data holder if technical protection measures or technical and organisational measures for the protection of business secrets[207] are changed or cancelled or not maintained. The rights of the data holder pursuant to Art. 11 DA cannot be deviated from to the detriment of the data holder (Art. 12(12) DA).

c) Use of the data by users

The Data Act pursues a user-related concept - the user bears the risks of using connected products and utilising related services and should therefore also benefit from their digitalised user actions, which are

---

201 Translated from Hennemann, M., et al, Data Act, p. 131; Antoine, L., *CR* 2024, 73 (77); Specht-Riemenschneider, L., *MMR* 2022, 809 (822) et seq.
202 Specht-Riemenschneider, L., *MMR* 2022, 809 (823).
203 For the latter 3 b) ee).
204 See 2 c) aa).
205 Specht-Riemenschneider, L., *MMR* 2022, 809 (821).
206 Specht-Riemenschneider, L., *MMR* 2022, 809 (821).
207 See c.5 c).

represented by IoT data.[208] Users must therefore have a claim against the holders of the data to the provision of the same to themselves or to third parties.[209] Conceptually, the Data Act pursues a **dual data access model** for the user: Data access is either by virtue of (technical) design (Art. 3(1) DA) or at the simple request of the user by electronic means (Art. 4(1) DA). Access can mean, for example, the transmission of a copy of the data or a transmission in real time.[210] With regard to the issue of access rights, the distinction between intentional and indirect generation of data is irrelevant; even data generated during inactivity is subject to the requirements of usability.[211] However, data that has been derived, for example by combining several sensor signals into an overall image, is exempt from this requirement. The interpretation through such a combination creates its own added value (worthy of protection).[212]

The Data Act does not explicitly regulate any specific data usage authorisations for users.[213] However, the user should be free to use the data for any lawful purpose.[214] The user may even pass the data on to third parties.[215] According to Art. 4(10) DA, however, there is a non-compete obligation on the primary market with regard to the data obtained.[216]

Small and medium-sized enterprises (SMEs) are exempt from the obligation to utilise the data in accordance with Art. 7(1) DA.

To summarise, the user - unlike the data holder - is not subject to any restrictions when using the data, provided the data is not used for the development of competing products or the data holder's business secrets are not affected.

aa) Data access *by design*, Art. 3(1) DA

According to Art. 3(1) DA, connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format. Where relevant and technically feasible, direct access must be provided.

Unlike most other obligations under the Data Act, the design obligation under Art. 3(1) DA applies to the manufacturer, who is not necessarily the subsequent data holder.[217] As there does not have to be a contract between the manufacturer and user, Art. 3(1) DA creates a legal obligation.[218] So-called *by-*

208 Rec. 18 Regulation (EU) 2023/2854; Funk, A., *CR* 2023, 421 (421) et seq.
209 Rec. 18 Regulation (EU) 2023/2854.
210 Hennemann, M./Steinrötter, B., *NJW* 2024, 1 (3).
211 Specht-Riemenschneider, L., *MMR* 2022, 809 (815).
212 See Rec. 15 Regulation (EU) 2023/2854; Hennemann, M./Steinrötter, B., *NJW* 2024, 1 (3).
213 Heinzke, P., *BB* 2023, 201 (207).
214 Rec. 30 Regulation (EU) 2023/2854.
215 Translated from Hennemann, M., et al, Data Act, p. 76 et seq.
216 Wiebe, A., *CR* 2023, 777 (778).
217 Assion, S/Willecke, L., *MMR* 2023, 805 (805); Steinrötter, B., *GRUR* 2023, 216 (220).
218 Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (52).

design regulation models are already familiar from European data protection law.[219] In light of this, however, there are considerable differences: unlike Art. 25(1) GDPR, for example, Art. 3(1) DA does not intend to protect against risks to the rights and freedoms of natural persons through the technical design of connected products and related services.[220] Rather, Art. 3(1) DA establishes a **legal model** in the sense of a *default*[221] for efficient data access: in the best case scenario, users should be able to retrieve the relevant product and related service data from the corresponding product or service without any further intermediate step.

The so-called ***accessibility-by-design regulation*** in the Data Act is therefore a completely new instrument, the practical effects of which are difficult to predict. However, the vagueness of the data access modalities could mean that the product concept does not change significantly.[222] This is particularly true because Art. 3(1) DA makes direct data access dependent on technical feasibility. However, Art. 3(1) DA does not specify when direct data access is technically feasible. Technical feasibility can therefore be regarded as a legal and factual limit to data access *by design*, which is likely to weaken rather than strengthen the position of the user.[223]

Finally, the data must be available in the same quality as for the data holder, at the latest upon request of the user (Art. 4(1) DA).[224] Unlike Art. 4(1), 5(1) DA, Art. 3(1) DA does not regulate access to data in real time.[225]

(1) Legal consequences of a breach of duty

The legal consequences of a breach by manufacturers of their legal obligations under Art. 3(1) DA remain unclear. These arise implicitly from national contract law.[226] Since the standard does not contain any provisions on this either, the burden of proof for a breach of the standard is probably on the user in accordance with the general provisions.[227] This suggests that the standard is merely appellative in nature.[228] A judicial review of the obligation under Art. 3(1) DA could ultimately be limited to proven violations: Deleting the data before the user can request access in accordance with Art. 4(1) DA would undoubtedly be in breach of duty.[229] In essence, Art. 3(1) DA is therefore intended to protect the enforceability of data access claims under Art. 4 et seq. DA.

---

219 v. Lewinski, K., 'GDPR Art. 20', in: BeckOK Datenschutzrecht, para. 117c.
220 Paulus, E.-M., 'GDPR Art. 25', in: BeckOK Datenschutzrecht, para. 7.
221 Hennemann, M./Steinrötter, B., *NJW* 2022, 1481 (1483).
222 Gerpott, T., *CR* 2022, 271 (275).
223 Kaesling, K., *GRUR* 2024, 821 (823).
224 Antoine, L., *CR* 2024, 1 (5).
225 Antoine, L., *CR* 2024, 1 (5).
226 Hennemann, M./Steinrötter, B., *NJW* 2022, 1481 (1483).
227 BGH, judgement of 13. 11. 1998 - V ZR 386-97, *NJW* 1999, 352 (353).
228 Gerpott, T., *CR* 2022, 271 (275); Specht-Riemenschneider, L., *MMR* 2022, 809 (815).
229 Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (52).

According to Art. 7(1)(d) Directive 2019/771/EU[230] (or Art. 8 (1)(b) Directive 2017/770/EU), the seller of a product designed in violation of Art. 3(1) DA could be held liable for defects.[231] According to Art. 18 Directive 2019/771/EU[232], the seller would in turn be able to take recourse up to the manufacturer.[233] Due to the vagueness of Art. 3(1) DA and the linking of Art. 7(1)(d) Directive 2019/771/EU to what can reasonably be expected, customary practice is of great importance here. Only the European Court of Justice can ultimately clarify what is to be understood by this in individual cases. Because Art. 3(1) DA can be seen as a rule of market behaviour,[234] liability under competition law pursuant to § 3a UWG is also conceivable.[235]

(2) Direct access where relevant and technically feasible, Art. 3(1) DA

In instances where relevant and technically feasible (Art. 3(1) DA), the user must be granted direct access by the manufacturer. If direct access is not relevant and feasible, the data access claim pursuant to Art. 4(1) DA applies. Direct data access and the right to data access are mutually exclusive.[236] The data access claim is also the legal consequence of a breach of a direct access obligation pursuant to Art. 3(1) DA.[237]

Direct access in accordance with Art. 3(1) DA must not be misunderstood as an assignment of the data to the user. The data is and remains technically and factually assigned to the data holder by the Data Act; the data holder continues to have so-called *de facto control* over the data.[238] Rather, the de facto control of the data holder is limited by the provisions in favour of the user, even though the user must take action himself to exercise his rights.[239] The legislator assumed that data would only be made available if the user actually requested access.[240] Models such as easy-to-use[241] user interfaces or the storage of data on user-accessible servers or the device itself are possible.[242] The Data Act leaves unanswered the question of which view is relevant for categorising access as direct in accordance with Art. 3(1) DA. Depending on whether it is the average user in the form of a consumer or the technically qualified expert that is relevant, the legal consequence, i.e. the mode of access to be granted, differs considerably.[243]

230 The standard was implemented in German law in Section 434(3) BGB.
231 Antoine, L., *CR* 2024, 1 (5); Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (52); on the applicability of the Sale of Goods Directive in general Drexl et al, Data Act, para. 74.
232 Implementation in German law in § 445a BGB.
233 Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (52).
234 Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (52); cf. Drexl, J., et al, Data Act, (76).
235 Antoine, L., *CR* 2024, 1 (5); Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (52).
236 Heinzke, P., *BB* 2023, 201 (207); Specht-Riemenschneider, L., *MMR* 2022, 809 (815).
237 Specht-Riemenschneider, L., *MMR* 2022, 809 (815).
238 Rec. 5 Regulation (EU) 2023/2854; Antoine, L., *CR* 2024, 1 (2); Specht-Riemenschneider, L., *MMR* 2022, 809 (815).
239 Müller, J., *RDi* 2024, 297 (303); Specht-Riemenschneider, L., *MMR* 2022, 809 (815).
240 Rec. Regulation (EU) 21 2023/2854.
241 Art. 3(1) DA.
242 Rec. 22 Regulation (EU) 2023/2854; Specht-Riemenschneider, L., *MMR* 2022, 809 (815).
243 DAV, Opinion 40/2022 on the draft Data Protection Act, p. 15.

What needs to be clarified is what relevance and technical feasibility mean within the meaning of Art. 3(1) DA.

The legislator has used a legal concept similar to technical feasibility in Art. 20(2) GDPR. According to this, data must be transmitted directly to a controller within the meaning of the GDPR insofar as this is technically feasible. As with Art. 20(2) GDPR, the obligation under Art. 3(1) GDPR is free of charge. Therefore, the legal term in question for objectively unusual modes of provision or data formats must be interpreted more narrowly.[244] On the other hand, the use of common file formats or low-friction provision via the internet, for example by cloud providers, objectively speaks in favour of technical feasibility.[245]

Subjective circumstances such as the size and capacity of the data holder (or controller) are increasingly being cited for considerations in the context of Art. 20(2) GDPR.[246] In any case, subjective aspects cannot be disregarded in the required overall assessment. However, they open up a very narrow case-by-case assessment that could make the enforceability and practical significance of the right to direct access under Art. 3(1) GDPR significantly more difficult.[247]

In addition, the characteristic of relevance must not be neglected. Direct data access should be considered particularly relevant where it is closely related to the purposes of data access: better use of devices or services,[248] the strengthening of a secondary market in favour of users,[249] the promotion of innovation[250] and the development of a new data economy.[251]

(3) Duty to inform, Art. 3(1), (2),(3) DA

The data holder's duty of conception (Art. 3(1) DA) is flanked by extensive information obligations pursuant to Art. 3(2) and (3) DA. The user has a claim against the contractual partner to a pre-contractual, one-off provision of information. The information that must be provided prior to the conclusion of the contract depends on whether it is a contract for connected products (Art. 3(2) DA) or related services (Art. 3(3) DA). In most cases, the user's contractual partner will be a (wholesale) trader, not the data holder itself.[252] In particular, it is essential for the enforcement of other user rights that the contractual partner informs the user of the identity of the data holder.[253] In practice, compatibility with consumer contract law, which is not affected by Art. 1(9) DA, could prove difficult.[254]

---

244 v. Lewinski, K., 'GDPR Art. 20', in: BeckOK Datenschutzrecht, para. 88.
245 Correspondingly to Art. 20 GDPR: v. Lewinski, K., 'GDPR Art. 20', in: BeckOK Datenschutzrecht, para. 88.
246 v. Lewinski, K., 'GDPR Art. 20', in: BeckOK Datenschutzrecht, para. 88.
247 See on Art. 20 GDPR Antoine, L., *CR* 2024, 1 (5).
248 Kaesling, K., *GRUR* 2024, 821, 821.
249 https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet; Kerber, *GRUR Int.* 2023, 120 (122).
250 Kerber, W., *GRUR Int.* 2023, 120 (122).
251 Heinzke, P., *BB* 2023, 201 (202) et seq.
252 Wilkening, P./Müller, J., *DB* 2024, 166 (169).
253 See Ehlen, T./Sebulke, P. *CR* 2024, 84 (89).
254 Ehlen, T./Sebulke, P., *CR* 2024, 84 (89).

bb) Data access claim of the user for readily available data, Art. 4 DA

Pursuant to Art. 4(1) DA, the data holder is obliged, at the request of the user, to provide the user with the readily available data if the user cannot obtain it directly from the product or service (Art. 3(1) DA). A transfer of the statutory data access claim is not possible in accordance with its meaning and purpose.[255]

(1) Provision modalities

The provision must be simple, secure, free of charge and, where relevant and technically feasible, continuous and in real time. As far as possible, data must be provided in the same quality as for the data holder.[256] The legal terms used must be interpreted independently of national law.[257]

It does not matter whether the data is actually made available to the user or whether access to a computer belonging to the data holder is set up.[258] However, this so-called **in-situ access**[259] means a significant additional effort for the user.[260] Continuous real-time in-situ access would probably be easy for the data holder to realise. On the other hand, application programming interfaces (APIs) offer direct access and are also preferable in terms of interoperability.[261] As a result, in-situ access should therefore be possible, but the exception. Otherwise, the promotion of innovation and a secondary data economy would be significantly hindered.[262] This position is further reinforced by the specific wording of recital 22, which uses the permissive form "may". In addition, in-situ solutions harbour the risk that the data holder monitors the use of the data on its server and gains competitive advantages over users and third parties.[263] A judicial clarification to the effect that in-situ provision is regarded as the standard model also appears conceivable.[264]

(2) Concept of readily available data

As with the requirement for a user agreement (Art. 4(13) DA),[265] the right to data access is linked to the legal concept of **readily available data** (Art. 2 No. 17 DA).[266] The user can only request access to such data in accordance with Art. 4(1) DA. It can be concluded from the parallel that data used by the data holder can be the subject of a request for access.

Concerning the second alternative of readily available data under Art. 2 No. 17 DA, issues of certainty emerge, specifically in relation to the data that the data holder is capable of obtaining. In this case, as

---

255 Wiebe, A., *GRUR* 2023, 1569 (1572).
256 Assion, S./Willecke, L., *MMR* 2023, 805 (807).
257 Translated from Hennemann, M., et al, Data Act, p. 87; Schmidt-Kessel, M., *MMR* 2024, 75 (79).
258 Rec. 22 Regulation (EU) 2023/2854.
259 The idea of an in-situ access right was developed by Martens, B./Parker, G./Petropoulos, G./Van Alstyne, M., Towards Efficient Information Sharing in Network Markets, *TILEC DP* 2021-014, p. 4.
260 See Drexl, J., et al, Data Act, (66); Specht-Riemenschneider, L., *MMR* 2022, 809 (816).
261 Translated from Hennemann, M., et al, Data Act, p. 88.
262 Kaesling, K, *GRUR* 2024, 821 (825).
263 Kerber, W., *GRUR Int.* 2023, 120 (124).
264 For example Kaesling, K., *GRUR* 2024, 821 (824); Kerber, W., *GRUR Int.* 2023, 120 (124).
265 See bullet point b) aa).
266 For the definition, see 2 c) aa) (6).

opposed to the first alternative and thus also in the context of Art. 4(13) DA,[267] the characteristic of not disproportionately high effort is important. This is because the user should also be able to request access to data that the data holder has not yet received, but can do so without disproportionate effort.[268] What constitutes a disproportionate effort can only be determined on a case-by-case basis.

In addition, as in the context of Art. 4(13) DA, data that was not designed to be stored or transmitted outside the component generating it or the product as a whole is excluded.[269]

A restriction of access can only be contractually agreed if the processing of the data affects the legally defined safety requirements of the connected product and this could lead to serious effects on the health or safety of natural persons, Art. 4(2) DA. In the event of a complete refusal of disclosure by the data holder, the data holder must inform the competent authority (Art. 37 DA). The user can lodge a complaint against unauthorised restrictions (Art. 4(3)(a) DA) or agree that a dispute resolution body will deal with the matter (Art. 4(3)(b) DA).

The exercise of the rights under Art. 4 DA must not be made unreasonably difficult for the user by the data holder. An unreasonable impediment exists, among other things, if the user is offered choices in a non-neutral manner, Art. 4(4) DA.

(3) Separation of producer and data holder

Data holders and manufacturers are usually, but not always, identical.[270] It is unlikely that data will be generated by a connected product and collected in a system that is controlled by a third-party data holder who is not the manufacturer.[271] If the manufacturer and data holder are not identical, the following problems arise:

According to the legal definition in Art. 2 No. 13 DA, the data holder can be anyone who is only authorised to use the data but cannot provide it. In order to hand over the data to the user, which the data holder is obliged to do at the request of the user in accordance with Art. 4(1) DA, the technical support of the manufacturer may be required.[272] However, the Data Act does not contain an explicit obligation for the manufacturer to do so.[273]

It is possible that the characteristic of availability will now become significant without further ado. Data that the holder can only obtain with the assistance of the manufacturer, but which the latter refuses to provide due to a lack of legal obligation, would not be readily available under Art. 4(1) DA. Therefore, the data holder would not be obliged to hand it over. However, this would mean that the loophole in the Data Act would be to the detriment of the user. The manufacturer could evade a data disclosure claim

267 See bullet point b) aa).
268 See Rec. 20 Regulation (EU) 2023/2854.
269 Rec. 20 Regulation (EU) 2023/2854.
270 Kerber, W., *GRUR Int.* 2023, 120 (123); Steinrötter, B., *GRUR* 2023, 216 (219).
271 Podszun, R./Pfeifer, C., *GRUR* 2022, 953 (956).
272 DAV, Opinion 40/2022 on the draft Data Protection Act, p. 15.
273 DAV, Opinion 40/2022 on the draft Data Protection Act, p. 15.

by using a data holder without the possibility of making the data available. In the sense of a secondary market, as intended by the Data Act, this could[274] not be intended by the legislator.

A broad interpretation of Art. 3(1) DA could offer a solution: For example, it could be argued that a model that immediately fulfils the user's rights excludes comprehensive access by the user, but that this would have to be taken into account in the production and design in accordance with Art. 3(1) DA. As a legal consequence, recourse by the user to the manufacturer or a (third-party) effect of the standard in the relationship between the manufacturer and the data holder would be conceivable in individual cases. If the manufacturer transfers data management to a data holder, this is usually done on the basis of a contract. An enabling obligation could be inferred from this by interpreting it in the light of Art. 3 (1) DA.

Ultimately, it is highly unlikely that uncertainties will arise to the detriment of the user in circumstances where producers and data holders diverge, due to the unambiguous nature of the Data Act, at least in terms of its aim of ensuring the free flow of data.[275]

(4) Checking the user status

If a person requests access to data in accordance with Art. 4(1) DA, the data holder must check whether they are also the user within the meaning of Art. 2 No. 12 DA. However, the data holder may only request the necessary information for this purpose (Art. 4(5) DA). This means that data holders may at least not make it difficult to establish the identity through active behaviour.[276] According to the recitals, user identification should generally take place via a user account.[277]

If several individuals are users within the meaning of Art. 4(1) DA, the effort required to establish identity increases.[278] In particular, checking which individual has generated the data in question through their use of a connected product or service (Art. 2 No. 15, 16 DA) can be very time-consuming.[279] This argues in favour of interpreting the concept of user more narrowly based on interests: in individual cases, it depends on who has a legitimate interest in the data.[280] For example, if an employee is travelling by car in his employer's car, only the latter would be a user within the meaning of Art. 4(1) DA.[281] In case of doubt, however, the legislator also considers cases of multiple users possible, for example in the case of car-sharing services.[282] According to Art. 4(5) DA, the data holder remains obliged to assess whether a legitimate interest exists.

---

274 European Commission, Data Law - Factsheet 2022; Kerber, W., *GRUR Int.* 2023, 120 (122).
275 Kerber, W., *GRUR Int.* 2023, 120 (122).
276 Gerpott, T. *CR* 2022, 271 (271).
277 Rec. 21 Regulation (EU) 2023/2854.
278 Antoine, L. *CR* 2024, 1 (4).
279 Antoine, L. *CR* 2024, 1 (4).
280 Drexl, J., et al, Data Act, para. 59.
281 Bomhard, D./Merkle, M., *RDi* 2022, 168 (170).
282 Rec. 18 Regulation (EU) 2023/2854.

Art. 4(5) GDPR is also related to Art. 4(12) GDPR. According to this, the data holder may also provide the user with personal data generated during the use of a connected product or related service if a valid legal basis pursuant to Art. 6 GDPR exists and, if applicable, the requirements of Art. 9 GDPR and Art. 5(3) ePrivacy Directive[283] are met. However, Art. 4(5) DA and Art. 4(12) DA do not contain any specific information on how the verification, including the examination of the legal basis, is to be carried out in accordance with the GDPR. The requirements for verification criteria require a proportionate balance to be struck between ease of access and the prevention of abuse. If the competent authorities set high requirements for verification in relation to both the Data Act and the GDPR, data holders will find themselves in an almost irresolvable conflict of objectives, as the following example illustrates: As part of the verification process, the data holder could require the user to scan their rental agreement and submit it via an app for verification, assuring that they are an authorised user. The data holder would then check the validity of the rental agreement, which is difficult and time-consuming in mass transactions. Only after a positive check result would the user be able to request data transfer; this check would have to be repeated regularly. This example illustrates that strict application of the Data Act and the GDPR could result in prohibitively high hurdles for the user, forcing them to refrain from requesting the provision of data.

(5) Handling of business secrets, Art. 4(6) – (9) DA

According to Art. 4(6) DA, **trade secrets** are protected and only disclosed if the data holder and the user have taken all measures necessary to protect the confidentiality of the trade secrets, in particular vis-à-vis third parties, prior to disclosure. The determination of which data are considered to be trade secrets is made by the proprietor of the trade secret (Art. 4(6) DA). In accordance with the provisions of the Data Act, the data holder is typically designated as the data proprietor.[284]

(a) Definition of trade secret

In accordance with Art. 2 No. 18 DA, the definition of a trade secret is based on Art. 2 No. 1 of Directive (EU) 2016/943 (Directive on the protection of confidential know-how and business information (trade secrets) against their unlawful acquisition and unlawful disclosure; hereinafter referred to as "Trade Secrets Directive"): Trade Secrets Directive). Accordingly, trade secrets are

> Information[s] that fulfil all of the following criteria:
>
> (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
>
> b) it has commercial value because it is secret;

283 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

284 Rec. 31 Regulation (EU) 2023/2854.

(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;

The conditions stated in the definition must be met cumulatively.

German law covers information of all kinds, including details, formulas and images.[285] The characteristic of secret information depends on the practical possibility of access for groups of people who usually process this type of information.[286] The economic value of information is determined by its relevance to economic or corporate strategy.[287]

(b) Burden of proof of the trade secret holder, Art. 4(6) DA

The data or trade secret holder identifies the data protected as a trade secret, Art. 4(6) DA. The disclosure requirements for the existence of such data are low, as premature publication of data classified as a trade secret can have serious economic and legal consequences. Under the Trade Secrets Directive, the requirements for demonstrating the existence of trade secrets for applications for procedural protective measures are also set low, meaning that a prima facie case would already exceed the requirements. It would be a contradiction in terms to set higher requirements for the presentation of trade secrets under the Data Act, which refers to the Trade Secrets Directive via Art. 2 No. 18 DA.[288]

(c) Disclosure under technical and organisational measures, Art. 4 DA

Data that constitutes business secrets may only be disclosed subject to the necessary **technical and organisational measures** (TOMs). This is intended to ensure that the confidentiality of business secrets is maintained, particularly vis-à-vis third parties.[289]

The TOMs required by the user to ensure confidentiality are the subject of an agreement between the data holder or the holder of the trade secret and the user, Art. 4(6) DA. The TOMs must meet the standards of appropriateness. The indeterminate legal concept of adequacy is concretised by standard examples (Art. 4(6) DA). The vagueness of the term also leads to uncertainties with regard to confidentiality agreements between data holders and data users.[290] It remains unclear who should draw up the confidentiality agreement and which modalities must be adhered to.[291] The question arises as to how far-reaching such agreements can be.[292] In practice, the model contractual clauses to be drawn up by the Commission in accordance with Art. 41 DA will be of decisive importance.[293]

285 Köhler, H./Bornkamm, J./Feddersen, C./Alexander, C., UWG, GeschGehG § 2 para. 25.
286 Ohly, *GRUR* 2019, 441 (443); Köhler, H./Bornkamm, J./Feddersen, C./Alexander, C., UWG, GeschGehG § 2 (33).
287 LAG Baden-Württemberg, judgement of 18 August 2021 - 4 SaGa 1/21 (37).
288 Pauly, D.A./Wichert, F./Baumann, J., *MMR* 2024, 211 (212).
289 Rec. 31 Regulation (EU) 2023/2854.
290 Holznagel, B./Freese, F., *EuZ* 2023, A 17; Bomhard, D./Merkle, M., *RDi* 2022, 168 (171).
291 Bomhard, D./Merkle, M., *RDi* 2022, 168 (171).
292 Lorenzen, B., *ZGE* 2022, 250 (265), is also critical with regard to confidentiality measures.
293 In this direction v. Roenne, H.,'DA Art. 41', in: BeckOK Datenschutzrecht, para. 15.

According to Art. 4(7) DA, the data holder has the right to refuse or subsequently suspend the disclosure of data classified as trade secrets. The prerequisite for this is that the agreed TOMs have not been adhered to, none were agreed in the first place or the confidentiality of the trade secret has nevertheless been breached. If the data holder decides to refuse or suspend the disclosure, it is obliged to duly justify its decision and to inform the user of this in writing without delay (Art. 4(7) DA). In addition, a notification must be issued to the designated competent authority in accordance with Art. 37 DA. This notification must include, among other things, information regarding the trade secret that has been compromised (Art. 4(7) DA).

A refusal of the data access request is also possible if the data holder can prove that, despite the agreement of the necessary TOMs in accordance with Art. 4(6) DA and compliance with them by the user, he would have to fear serious economic damage if the data were passed on (Art. 4(8) DA). The Data Act already assumes from its wording ("in exceptional circumstances") that a right of refusal under Art. 4(8) DA is the glaring exception. As a rule, the regime of Art. 4(6), (7) DA applies. Even in the event of a refusal pursuant to Art. 4(8) DA, the data holder must submit the reasoned decision to the user in writing and inform the designated competent authority pursuant to Art. 37 DA. In contrast to a refusal under Art. 4(7) DA, the reasons must be based on objective facts. As standard examples of this, Art. 4(8) DA cites the enforceability of the protection of trade secrets in third countries, the type and degree of confidentiality of the requested data and the uniqueness and novelty of the connected product.

Complaints and dispute resolution are admissible against the refusal of disclosure, Art. 4(9) DA.[294] The designated competent authority decides with effect for and against the parties whether and under what conditions the data will be disclosed. Art. 33 DA allows Member States to adopt supplementary provisions on the protection of trade secrets.[295]

cc) Prohibition of data misuse, Art. 4(10) DA

Art. 4(10) DA limits the use of data obtained. The user may not use the data received from the data holder in accordance with Art. 4(1) DA or pass it on to third parties in order to develop a connected product in competition with the contractual connected product. Furthermore, the user is prohibited from utilising or transmitting data for the purpose of drawing conclusions regarding the economic situation, assets and production methods of the manufacturer (of the contractual connected product).

However, commercial use of data by the user is not excluded per se. In principle, the user may use the data provided to him under Art. 4(1) DA for both commercial and non-commercial purposes.[296] Subject to compliance with the provisions of data protection law (Art. 1(5) DA), there is nothing to prevent the

294 For dispute resolution see e).
295 Lorenzen, B., *ZGE* 2022, 250, 266.
296 Antoine, L., *CR* 2024, 1 (5).

data from being commercialised. However, data obtained through the data access claim pursuant to Art. 4(1) DA may not be passed on to gatekeepers within the meaning of Art. 3 DMA.[297]

dd) Obligation to use devices or services in good faith, Art. 4(11) DA

Users may not gain access to data by coercive means or exploit gaps in the data holder's existing infrastructure to protect the data (Art. 4(11) DA). This means that the user does not have a so-called *right to hack*.[298] It is true that the prohibition standard is based on the provisions on trade secrets (Art. 4(6) –(9) DA). However, according to its wording, Art. 4(11) DA refers to all data. The provision thus manifests the recognition and protection of the data holder's *de facto control* over all generated data.[299]

In order to counteract violations of this obligation, the data holder can take technical protective measures (Art. 11(1) DA).[300]

d) Use by and provision of data to third parties

The term third party is not defined in the Data Act. However, it can be deduced from the definition of data recipient pursuant to Art. 2 No. 14 DA that a third party within the meaning of the Data Act is defined as an entity that acts for commercial, business, trade or professional purposes. The third party must not be a user, which follows from a reverse conclusion from Art. 5(1) DA ("Upon request by a user"). In contrast to the average user, the third party has an interest in processing the data and the means to do so.[301] By utilising the data, for example for the development of innovative products, the third party increases the overall economic potential of the data. The inclusion of third parties in the regime of the Data Act is therefore fundamental to the creation of a European data economy as the central objective of the regulation.[302]

aa) Provision of data only at the request of the user, Art. 8(4) DA

Third parties are generally prohibited from using the data[303], as outlined in Art. 4(13) DA: If the data holder is already prohibited from using readily available data without a contractual basis, this applies a fortiori to third parties not involved in the original value creation process. Furthermore, the system of data access and use claims conclusively regulated in the Data Act also speaks in favour of a fundamental prohibition of use by third parties, as the European legislator has evidently dispensed with such an offence.[304]

297 Antoine, L., *CR* 2024, 1 (5).
298 See Specht-Riemenschneider, L. *MMR* 2022, 809 (821).
299 Drexl, J., et al, Data Act (116); Kerber, W., *GRUR Int.* 2023, 120 (124) et seq.
300 For technical measures within the meaning of the Data Act, section 3.b.cc.
301 Heinzke, P./Herbers, B./Kraus, M., *BB* 2024, 649 (650); Heinzke, P., *BB* 2023, 201 (204).
302 Heinzke, P. *BB* 2023, 201 (202) et seq.
303 On the argumentum a fortiori in the methodology of Union law Martens, Methodenlehre des Unionsrechts, p. 327 et seq.
304 See also Hennemann, M./Steinrötter, B., *NJW* 2024, 1 (7).

The data initially belongs to the user.[305] However, data holders, who generally have de facto control over the data,[306] can make the data available to third parties. This must either serve the "fulfilment of their contract with the user"[307] as a form of data use by the data holder (Art. 4(13) DA) or the user must have requested the provision (Art. 8(4) DA). If the user has obtained control over the data *by design* (Art. 3(1) DA) or by request (Art. 4(1) DA), they may disclose the data to third parties.

bb) Provision of readily available data to third parties at the request of the user, Art. 5(1) DA

At the request of a user, the data holder must make readily available data and the metadata required for its use available to a third party (Art. 5(1) DA). The user may request data access in favour of the third party that corresponds to their own data access.[308] Small and medium-sized enterprises are exempt from the obligation under Art. 7(1) DA.

(1) Modalities of provision, Art. 8 - 13 DA

If the user requests the provision of the data to a third party in accordance with Art. 5(1) DA, the modalities must comply with the requirements set out in Art. 8 et seq. DA must be complied with.

(d) Agreement of appropriate conditions, Art. 8(1) DA

For business relationships between companies in which a data holder undertakes to provide data (Art. 5(1) DA), the Data Act provides for an **obligation to contract.** As this only applies to business-to-business relationships according to the wording, Art. 8(1) DA cannot be applied if a consumer receives the data.[309] If a contract must be concluded in accordance with this provision, the structure for the provision of the data must be agreed. The data must also be provided to the data recipient on fair, reasonable and non-discriminatory terms and in a transparent manner.[310] The provision must also be in accordance with Chapter IV DA (Art. 8(1) DA). Art. 8(1) DA thus refers to the **control of general terms and conditions** according to Art. 13 DA.[311] Since a full review of agreed terms and conditions against the GTC and FRAND standards would be both impracticable[312] and generally too broad[313], the relationship between the review standards requires special consideration. Art. 13 DA sets substantive requirements on which the effectiveness of the contractual clauses depends.[314] However, these requirements only apply if the clauses were imposed unilaterally (Art. 13(1) DA); there is no such restriction in Art. 8(1) DA. A substantive review based on the **FRAND criteria** would therefore mean a massive

---

305 Rec. 18 Regulation (EU) 2023/2854; Hennemann, M./Steinrötter, B., *NJW* 2024, 1 (7).
306 Rec. 5 Regulation (EU) 2023/2854; Antoine, L., *CR* 2024, 1 (2); Specht-Riemenschneider, L., *MMR* 2022, 809 (815).
307 Rec. 26 Regulation (EU) 2023/2854.
308 Wiedemann, N./Conrad, T./Salemi, S., *K&R* 2024, 157.
309 Wiedemann, N./Conrad, T./Salemi, S., *K&R* 2024, 157 (162).
310 See also Rec. 42 Regulation (EU) 2023/2854.
311 See chapter 5.
312 In favour of an effect dampening the dynamic efficiency of data markets Picht, Mandatory Data Access Transactions, p. 29; Wiebe, A., *GRUR* 2023, 1569 (1573).
313 Antoine, L., *CR* 2024, 1 (7).
314 Translated from Hennemann, M., et al, Data Act, p. 141.

restriction of contractual freedom. However, the legislator wanted to leave the parties free to negotiate the provision modalities in the spirit of private autonomy.[315] The FRAND criteria are therefore not designed as substantive effectiveness requirements, but as procedural requirements for the negotiation of conditions as a basis for negotiation or guidance for decisions by dispute resolution bodies (Art. 10(1) DA), courts or authorities.[316] If a negotiation fails and, as a result, data is not provided in accordance with Art. 5(1) DA, an authority or court should be able to enforce the provision of data in accordance with FRAND standards.[317] In its *Huawei decision* on telecommunications technology patents, the ECJ set out several FRAND procedural requirements such as information and consultation obligations for patent holders.[318] It is unlikely that details of the decision will be applied. However, it can be assumed that the ECJ will also develop procedural requirements for Art. 8(1) DA.[319]

Art. 8(2) DA declares unfair terms within the meaning of Art. 13 DA to be non-binding.[320] This could also be the case if the clause was not determined unilaterally.[321] However, Art. 8(2) DA would only apply – even if not expressly so stipulated – to data provision that is mandatory under EU law, for example under Art. 5 DA, but not to voluntary provision.[322] This would leave Art. 13 DA with its own scope in line with the intention of the legislator, even if this is very limited. Understood in this way, Art. 8(2) DA is therefore a partial reference to a legal basis.

Bearing in mind the importance of private autonomy in EU law and the element of unilateral imposition, an interpretation as a complete reference[323] to all requirements of Art. 13 DA, including unilateral imposition, also appears conceivable. From a systematic point of view, the fact that the preceding first paragraph deals with the FRAND criteria suggests that Art. 8(2)(1) DA does not establish an independent standard of review, but declares unfairness to be an additional FRAND criterion.[324] This means that dispute resolution bodies are primarily addressed.[325]

According to Art. 8(2) DA, the user rights from Art. 3 to 7 DA may not be deviated from to the detriment of the user.

In Art. 8(1) DA, the Regulation refers to the data recipient instead of the third party as in Art. 5(1) DA. This is due to the literal applicability of Art. 8(1) DA to data provision claims from other legal sources.

315 Rec. 43 Regulation (EU) 2023/2854.
316 Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (70); *Wiebe*, A., GRUR 2023, 1569 (1573).
317 Drexl, J., et al, Data Act (101); Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (70) et seq.; cf. Rec. 42 Regulation (EU) 2023/2854.
318 CJEU, 16 July 2015, case C-170/13, para. 51-68 - Huawei Technologies/ZTE= CJEU *NJW* 2015, 2783.
319 Drexl, J., et al, Data Act (102); Translated from Hennemann, M., et al, Data Act, p. 115 et seq.
320 See also chapter 5 below.
321 Wiebe, A., GRUR 2023, 1569 (1573); see also Drexl, J. et al, Data Act (128).
322 Translated from Hennemann, M., et al, Data Act, p. 116.
323 See Rec. 59 Regulation (EU) 2023/2854.
324 Drexl, J., et al, Data Act, para. 128; Schwamberger, S., *MMR* 2024, 96 (97).
325 Cf. Drexl, J., et al, Data Act, para. 101, 128.

In the context of a consideration of Art. 8(1) DA in the typical constellation of persons under the Data Act, data recipient and third party can therefore be used practically synonymously.

(e) Prohibition of discrimination, Art. 8(3) DA

The data holder is prohibited from discriminating between comparable categories of data recipients by changing the respective modalities of data provision (Art. 8(3) DA). The data recipient who feels discriminated against by the modalities provided by the data holder must be provided with information immediately upon his justified request, which shows that there is no discrimination (Art. 8(3) DA). The burden of proof lies with the data holder, as the data recipient generally has no insight into the typical structures and modalities of the data holder's provision.[326]

(f) Consideration for the provision of data, Art. 9 DA

Art. 9 DA enables the data holder to agree a **consideration for the provision of the data.** This must be non-discriminatory and reasonable. The consideration may also include a margin, i.e. go beyond the actual costs of providing the data (Art. 9(1) DA). The consideration may be of a monetary nature, but is not limited to this.

The requirements for non-discrimination can be taken from Art. 8(3) DA.[327]

The Data Act also does not define what constitutes appropriate consideration. In addition to the measures in Art. 6(2), (3) DA, comparable market prices or market-oriented approaches from practice can also be used for orientation when determining an appropriate consideration.[328] This means that the consideration can be based on circumstances such as product development costs, contributions to the generation of the data concerned (both Art. 9(2)(b) DA) or the scope of the data (Art. 9(3) DA).[329] It is true that Art. 9 DA does not set a framework for the amount of the consideration, so that this could be unlimited in both directions. However, the requirements of Art. 9 DA prohibit overcompensation, meaning that compensation can only be demanded for the provision of the data itself.[330] The scope of the compensation can also be limited by regulations of the member states or the Union in accordance with Art. 9(6) DA. This means that the criterion of reasonableness in the context of Art. 9(1) DA is more specific than for the agreement of the provision modalities according to Art. 8 DA.[331]

In the context of the consideration, small and medium-sized enterprises are also relieved.[332] For them, the consideration may not exceed the costs of providing the data, including and in particular the necessary costs for formatting the data, processing by electronic means and storage (Art. 9(2)(a) DA), Art. 9(4) DA. The same applies to non-profit research organisations. According to Art. 9(7) DA, the data

326 Translated from Hennemann, M., et al, Data Act, p. 117.
327 Translated from Hennemann, M., et al, Data Act, p. 121; see section d) bb) (1) (b).
328 Translated from Hennemann, M., et al, Data Act, p. 120.
329 Antoine, L., *CR* 2024, 1 (7).
330 Translated from Hennemann, M., et al, Data Act, p. 119 - 121.
331 Antoine, L., *CR* 2024, 1 (7).
332 Translated from Hennemann, M., et al, Data Act, p. 121.

holder is obliged to provide the data recipient with information that enables him to verify the calculation of the consideration and compliance with the requirements of (1) – (4).

(g) Handling of business secrets (Art. 8(6) DA)

The obligation to provide data does not automatically oblige the disclosure of trade secrets (Art. 8(6) DA). The standard is viewed critically in light of the incentives it creates for the data holder to thwart data access.[333]

(2) Obligations of third parties who receive data at the user's request (Art. 6 DA)

Third parties who have received data at the user's request are subject to the obligations set out in Art. 6 DA. The provisions in Art. 6 DA are partially mandatory, Art. 7(2) DA. This seems inappropriate, as the potentially most powerful third parties, gatekeepers within the meaning of the DMA, are not addressees of the norm from the outset and users can also be entrepreneurs above the SME threshold.[334] However, the wording of Art. 6 DA does not provide a differentiation criterion.

Whether the respective provisions in Art. 6 DA constitute mandatory law must be determined by way of interpretation, in the context of which the meaning and purpose of the provision is of decisive importance.[335] Art. 6(1), (2)(a), (b) DA are probably mandatory.[336] On the other hand, it is not clear why the user should not be able to dispense with the protection of Art. 6(1), (2)(c), (f) DA. These provisions are therefore dispositive.[337] Since otherwise the purpose of Art. 5(3) DA would be undermined, Art. 6(2)(d) DA should be a mandatory provision.

(a) Individual obligations of the third party

Like the user, the third party may not use coercive means or exploit loopholes in protection in order to gain access to data (Art. 5(5) DA). According to Art. 6(1)(a) DA, the third party is obliged not to make it excessively difficult for the user to exercise his rights under Art. 5 and 6 DA, for example by deception or manipulation. This provision is intended to provide far-reaching protection for the autonomy of the user.[338]

The third party is prohibited from using the data provided for profiling purposes, with the exception of the necessity to provide the service requested by the user (Art. 6(2)(b) GDPR). This is specified in recital 39, which states that processing activities must be strictly necessary to provide the service, including in the context of automated decisions.

The third party is obliged not to use the data received to develop a product that is in competition with the product from which the data originates or to pass the data on to other third parties for this purpose.

---

333 Translated from Hennemann, M., et al, Data Act, p. 118 et seq.
334 Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (60).
335 Möslein, F., Dispositives Recht, p. 179.
336 Metzger, A./Schweitzer, H.,, *ZEuP* 2023, 42 (60).
337 Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (60).
338 Translated from Hennemann, M., et al, Data Act, p. 113.

The product data may also not be used to gain insights into the economic situation or production methods of the holder (Art. 6(2)(e) DA). However, innovative connected products or related services may be developed using the data provided as long as no competing connected product is developed as a result.[339] In this way, the promotion of innovation on the aftermarket is encouraged.[340] However, it remains unclear in several respects when a **competing connected product** is involved: for example, the question arises as to whether data from a refrigerator may be used for the development of an icebox, whereby this problem also arises analogously for the use of data from a car for the development of a lorry. It is also unclear whether data from a discontinued model may be used for the development of a future model. Furthermore, it remains unclear whether data from a product manufactured within the EU can be used for a comparable product in a third country, such as China.[341] Similar uncertainties exist with regard to the use of data from a conventional product for the development of a product based on artificial intelligence or for the mere improvement of a competing product. Finally, the question arises as to whether a review of the origin of the data is necessary in the context of a company acquisition.

Art. 6(2)(f) DA obliges the third party to ensure that the use of the data does not adversely affect the security of the connected product or related service.

In addition, the third party is obliged to take all measures agreed in accordance with Art. 5(9) DA to protect business secrets and to maintain the confidentiality of business secrets (Art. 6(2)(g) DA).

The Data Act standardises an obligation for the third party to delete data in Art. 6(1) GDPR; this is based on Art. 17 GDPR. The third party is obliged to erase the data as soon as it is no longer required to fulfil the agreed purpose.[342]

(b) Re-disclosure of data to other third parties, Art. 6(2)(c) DA

In principle, third parties are prohibited from passing on the data to another third party, unless the provision is based on a contractual agreement with the user (Art. 6(2)(c) DA). In addition, the other third party must also take all necessary measures to ensure the confidentiality of business secrets (Art. 6(2)(c) DA). Art. 6(2)(d) DA imposes the obligation not to disclose data to gatekeepers within the meaning of Art. 3 DMA. Thus, the prohibition of disclosure from Art. 5(3) DA is stringently continued.[343] However, it can be deduced from the system of Art. 6 that Art. 6 (2)(c) DMA exclusively refers to the data that is made readily available in accordance with Art. 5(1) DMA.[344] If the data holder himself provides data to third parties, he *may* contractually oblige them not to disclose the data again (Art. 4(14) DA). The wording of the provision ("where appropriate" instead of, for example, "the data holder may") suggests that there may be an obligation to enter into such a contractual agreement when sharing data. In any case,

339 Rec. 39 Regulation (EU) 2023/2854.
340 Translated from Hennemann, M. et al, Data Act, p. 112.
341 Similarly, Lorenzen, B., *ZGE* 2022, 250 (261).
342 Rec. 39 Regulation (EU) 2023/2854; Translated from Hennemann, M. et al, Data Act, p. 113.
343 Translated from Hennemann, M. et al, Data Act, p. 112.
344 See Art. 6(1) DA, which states "A third party shall process the data provided to it in accordance with Article 5".

the standard emphasises that Art. 6(2)(c) DA cannot apply to direct transfers by the data holder on the basis of the contract with the user. It seems logical to assume an obligation to agree on a prohibition of disclosure if the contract with the user does not contain any authorisation for repeated data disclosure. However, it is not necessary to expressly provide for repeated disclosure. For example, the contractual authorisation of the data holder to sell the data by the user would probably imply that the data acquirer may freely use the data, i.e. also pass it on.[345]

(3) Exclusion for gatekeepers (Art. 5(3) DA)

Companies that have been designated as **gatekeepers** in accordance with Art. 3 DMA are excluded from this possibility.[346] According to Art. 5(3)(b) DA, they are not authorised to request users to provide data to them within the meaning of Art. 5(1) DA; the same applies to data access according to Art. 4(1) DA. On this point, the Data Act admittedly lacks stringency and regulatory density, as there is no provision for a ban on gatekeepers receiving (directly) accessible data from users *by design* (Art. 3(1) DA). There is also no prohibition on the direct transfer of data from the data holder to a gatekeeper.[347]

Gatekeepers are companies with a significant influence on the internal market that provide a centralised platform service that serves as the main gateway for commercial users to access end users and that have an established and lasting position with regard to their activities or it is foreseeable that they will attain such a position in the near future (Art. 3(1) DMA). Which companies are to be considered gatekeepers within the meaning of the DMA is determined by the Commission by way of designation (Art. 3(1) DMA). These currently include *'Amazon'* (central platform service provided: *'Amazon'* and *'Amazon Marketplace'*) and *'ByteDance'* (central platform service provided: *'TikTok'*).[348] Consequently, even at the request of a user, data may not be provided by the data holder to the (still) six gatekeepers designated by the Commission.

The exclusion for gatekeepers is based on the view that it is disproportionate to grant data access to companies that already have a unique ability to acquire data.[349] In addition, data access would hinder the fair distribution of data value creation in the market.[350]

Before a company is appointed as a gatekeeper, a market investigation is carried out in accordance with Art. 17 DMA. If a company is then appointed as a gatekeeper, a review of the gatekeeper status must be carried out at least every three years in order to ensure legal certainty for all market participants, including the gatekeepers.[351]

---

345 For consent to resale, bullet point b) aa).
346 Translated from Hennemann, M., et al, Data Act, p. 106 et seq.
347 Drexl, J., et al, Data Act, para. 92.
348 https://ec.europa.eu/commission/presscorner/api/files/document/print/de/ip_23_4328/IP_23_4328_DE.pdf.
349 Rec. 40 Regulation (EU) 2023/2854.
350 Rec. 40 Regulation (EU) 2023/2854. The exclusion for gatekeepers was very controversial during the legislative process; in favour, for example, Drexl, J., et al, Data Act, para. 91; against this, for example, Krämer, J., Effectiveness of data sharing obligations, p. 25 et seq.; Kerber, W., *JoAE* 2024, 1 (6).
351 Rec. 30 Regulation (EU) 2022/1925.

In practice, the ban on passing on usage-generated data to gatekeepers can lead to difficulties for other data holders. A great deal of (organisational) effort is required to ensure that usage-generated data is not transmitted back when using the platform services provided, for example in the event of maintenance by a gatekeeper.[352] Users' rights will also be severely curtailed, as they will no longer be able to freely choose third-party service providers.[353] This is detrimental to the publicly proclaimed goal of strengthening a secondary market for the benefit of users.[354] The comprehensive exclusion of gatekeepers may also harm innovation due to a lack of competition[355] – a declared aim of the Data Act.[356] Since the exclusion for gatekeepers only covers their access to data as third parties within the meaning of Art. 5(1) DA, not as data holders, Art. 5(3) DA may also lead to gatekeepers buying up operators of connected products and further expanding their dominant market position.[357] On the other hand, it should be noted that while the possibilities of passing on data to gatekeepers of the user are massively restricted, data holders and manufacturers are not subject to any restrictions.[358] The extent to which the regulation is practicable therefore remains questionable.[359]

cc) Disclosure of data to third parties by the user himself

Cases are also conceivable in which the data is passed on directly from the user to the third party.

If a data holder is obliged to provide data to a third party in accordance with Art. 5(1) DA, it may demand non-discriminatory and appropriate consideration (Art. 9(1) DA). However, data contracts between the data holder and the user may not provide for any consideration (Art. 3(1), Art. 4(1) DA). The right to a consideration with a profit margin for the data holder could be circumvented if users and third parties work together (collusively) in that the user first requests the data from the data holder as an agency for the third party and then passes it on. Such cooperation could ultimately lead to a deviation from Art. 5(1), Art. 9(1) DA in favour of third parties and at the expense of the data holder.[360] On paper, this would not benefit the user either. This is because the user request required for the direct provision of data to a third party is also regularly based on a paid business relationship.[361]

On the other hand, the user should be free to provide the data to third parties.[362] Accordingly, the possibility of circumvention could have been intended by the legislator or was at least accepted: Since the

352 Wilken, T./Rammos, T., *DER BETRIEB*, 1241 (1243); Heinzke, P./Herbers, B./Kraus, M., *BB* 2024, 649 (655).
353 Drexl, J., et al, Data Act, para. 92.
354 European Commission, Data Law - Factsheet 2022; Kerber, W., *GRUR Int.* 2023, 120 (122).
355 Drexl, J., et al, Data Act, para. 92; Kerber, W., *JoAE* 2024, 1 (6).
356 Kerber, W., *GRUR Int.* 2023, 120 (122); Kerber, W., *GRUR Int.* 2023, 120 (130).
357 Drexl, J. et al, Data Act, para. 92; Kerber,W., *GRUR Int.* 2023, 120 (130).
358 Kerber, W., *JoAE* 2024, 1 (6).
359 Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (59) also expressed general criticism, proposing as a counter-proposal access for gatekeepers in return for opening up their data collections.
360 Bomhard, D./Merkle, M. *RDi* 2022, 168 (171); Holznagel, B./Freese, F., *EuZ* 2023, A 17; on the DA draft unchanged at this point Specht-Riemenschneider, L., *MMR* 2022, 809 (822).
361 Cf. Etzkorn, P., *RDi* 2024, 116 (121).
362 Rec. 30 Regulation (EU) 2023/2854.

data holder does not incur any additional expense, he can also be expected to waive his remuneration in accordance with Art. 9(1) DA. However, a restriction applies in any case to business secrets, the disclosure of which the data holder can prohibit (Art. 4(6), (7) DA), which could already protect the interests of the data holder.

There are also some indications that the maintain the possibility of users transferring data to third parties.[363] This is because Art. 5(39)(c) DA prohibits gatekeepers from receiving data that users have obtained in accordance with Art. 4(1) DA. Conversely, this means that direct provision of data by the user to non-gatekeepers is generally permissible.[364] This would also correspond to the user's fundamental freedom to use data for "any lawful purpose"[365].

In practice, the transfer of data by the user to third parties will likely only be feasible in exceptional circumstances. This is due to the fact that the process necessitates a well-developed technical infrastructure and equipment on the part of the user, and is generally likely to be particularly complex.[366]

Otherwise, no agreement between the data holder and the third party is required, as there is no obligation to provide data under Art. 5 DA or other law (Art. 8(1) DA).

e) Dispute resolution by dispute resolution bodies (Art. 10 DA)

Users, data holders and data recipients (third parties) have access to certified dispute resolution bodies in accordance with Art. 10(1) DA. **Dispute resolution bodies** are responsible for disputes regarding the scope of trade secret protection in the relationship between data holder and user and data holder and third party (Art. 10(1) in conjunction with Art. 4(9), 5(12) DA). In the relationship between the data holder and the user, recourse to a dispute resolution body can be agreed in the event of disputes over a refusal of data access pursuant to Art. 4(1) DA due to impairment of state-imposed security requirements (Art. 4(2), (3) DA). If a dispute arises between a third party and the data holder regarding the definition of FRAND conditions, both parties also have access to a dispute resolution body (Art. 10(1) DA). The parties are free to choose the dispute resolution body. Whether it is within or outside their Member State of establishment is irrelevant.[367]

Some argue that the competence of the dispute resolution bodies to examine the material aspects also extends to the question of *whether* a right to data access exists.[368] The main argument in favour of this is the amended wording of the standard compared to the Commission draft.[369] Nevertheless, both text versions of Art. 10(1) DA are almost identical and refer to the FRAND conditions according to Art. 8(1)

363 Holznagel, B./Freese, F., *EuZ* 2023, A 23 et seq.
364 Holznagel, B./Freese, F., *EuZ* 2023, A 24; see also Hennemann, M./Steinrötter, B., *NJW* 2022, 1481 (1484).
365 Rec. 30 Regulation (EU) 2023/2854.
366 Translated from Hennemann, M., et al, Data Act, p. 119; similarly Bomhard, D./Merkle, M. *RDi* 2022, 168 (173).
367 Rec. 53 Regulation (EU) 2023/2854.
368 Translated from Hennemann, M. et al, Data Act, p. 126; Weiß, R., *MMR* 2024, 101.
369 Weiß, R., *MMR* 2024, 101.

DA, and not to the "conditions" of a data access claim, due to the designation corresponding to Art. 8(1) DA.[370] The alleged text amendment can therefore only refer to the English version of the text, which originally read as follows in Art. 10(1) DA:

> "*disputes in relation to the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available*" and
>
> "*disputes relating to the fair, reasonable and non-discriminatory terms and conditions for, and transparent manner of, making data available*".

This makes the relevant change for the argument clear: the phrase "*conditions for* [...] *making data available*" is interpreted to mean that the legal requirements for the provision of data are also part of the subject matter of the dispute resolution bodies. However, this fails to recognise that Art. 10(1) DA refers to "*terms and conditions*". The legal term corresponds to the "*terms and conditions*" used in Art. 8(1) DA. In Art. 8(1) COM(2022) 68 FINAL, the term was still only "*terms*". The amendment in Art. 10(1) DA is therefore only intended to harmonise the standard with the amended Art. 8(1) DA. The terms "*terms and conditions*" and "*terms*" refer to the standardised FRAND terms in the German version.

In terms of substantive law, the legislator did not intend to change the English language version of Art. 10(1) DA with the editorial amendment. Consequently, the argument put forward in the literature does not hold water. The assessment of whether a data access claim exists under substantive law is not within the competence of the dispute resolution bodies.

The possibility of taking legal action against the decision of a dispute resolution body remains unaffected for all parties involved (Art. 4(3), (9), Art. 5(12), Art. 10(13) DA).[371] Furthermore, the decisions are only binding if the parties have expressly agreed this before the start of the proceedings (Art. 10(1)2 DA). This explains the purpose of the new procedure: the extremely labour-intensive and costly FRAND disputes would place an immense burden on the courts.[372] Dispute resolution bodies, on the other hand, are intended to be particularly efficient and cost-effective and,[373] similar to arbitration tribunals, relieve the burden on state courts.[374] The importance of procedural efficiency is expressed not least in Art. 10(7) and (9) DA.[375] An application that has already been submitted to another body or a member state[376] court must be rejected (Art. 10(7) DA). Decisions must be made within 90 days (Art. 10(9) DA).

---

370 This is also the case for the DA draft, translated from Hennemann, M., et al, Data Act, p. 126; Weiß, R., *MMR* 2024, 101.

371 Translated from Hennemann, M., et al, Data Act, p. 124.

372 Translated from Hennemann, M., et al, Data Act, p. 124.

373 See Art. 10(5)(d) DA and Rec. 52 Regulation (EU) 2023/2854.

374 Niedermaier, T./Picht, P. *EuZW* 2023, 1035 (1036).

375 Weiß, R., *MMR* 2024, 101, (102), (104).

376 It could also be argued that the wording of the standard ("court of a Member State") only refers to the Member State in which the dispute resolution body is located. However, due to the orientation of Art. 10 DA towards procedural efficiency, the term must refer to all Member State courts. See Weiß, R., *MMR* 2024, 101 (102).

The provision on the bearing of costs pursuant to Art. 10(3) DA is also advantageous for users and third parties. Fees or other costs charged by the dispute resolution body only have to be reimbursed to the data holder in the event of a decision unfavourable to them if they have acted in bad faith (Art. 10(3) DA). On the other hand, if a decision is made in their favour, they can demand reimbursement of the fees as well as all other reasonable expenses (Art. 10(3)DA). The parties must be informed of the amount of the fees in advance of the proceedings. This enables them to assess the financial benefits and risks of the proceedings at an early stage.[377] The fact that the cost-sharing regulation penalises the data holder could significantly reduce their willingness to agree to a dispute resolution procedure and thus damage the practical relevance of the mechanism.[378]

In order to be certified by a Member State, the dispute resolution body must be impartial, have the necessary expertise and be easily accessible by electronic means of communication (Art. 10(5)(a) – (c) DA). It must also be able to decide quickly, efficiently and cost-effectively in at least one official language of the Union (Art. 10(5)(d) DA). The Commission shall publish a list of all certified dispute resolution bodies (Art. 10(6) DA). In the Data Act Commission draft, Art. 10(2) COM(2022) 68 FINAL still provided for an obligation to set up dispute resolution bodies for Member States in the event that no dispute resolution body has yet been authorised in the Member State. This provision was deleted without replacement in the final version of the Data Act. As a result, there are no longer any provisions for state dispute resolution bodies.[379] However, state dispute resolution bodies are still possible – provided they fulfil the requirements of Art. 10(5) DA – in the absence of deviating provisions.[380] This is because, in principle, they can also fulfil the purpose of the proceedings before a dispute resolution body, i.e. efficient dispute resolution that relieves[381] the burden on the courts.[382]

4. Unfair contract terms unilaterally imposed on another company , Art. 13 DA

a) Background

Art. 13 DA regulates the handling of unfair contractual terms that are unilaterally imposed on a company. The background to the regulation stems from the potential for power imbalances among the parties subject to the provisions of the Data Act.[383] As part of their cooperation, which is partly voluntary and partly mandatory by law, the aim is to prevent one party from abusing its dominant market position.[384]

377 Translated from Hennemann, M. et al, Data Act, p. 126.
378 Translated from Hennemann, M. et al, Data Act, p. 127; Weiß, R., *MMR* 2024, 101 (104).
379 Weiß, R., *MMR* 2024, 101 (102).
380 Niedermaier, T./Picht, P., EuZW 2023, 1035, 1036; see also the wording of Rec. 52 Regulation (EU) 2023/2854.
381 Art. 10(5)(d) DA and Rec. 52 Regulation (EU) 2023/2854.
382 See Niedermaier, T./Picht, P., *EuZW* 2023, 1035 (1036).
383 Schwamberger, S., *MMR* 2024, (96).
384 Rec. 58 Regulation (EU) 2023/2854.

This idea is particularly evident in the fact that Art. 3 to 12 DA stipulates obligations that force competing companies to cooperate (obligation to contract) in order to fulfil the user's claims to the transfer of product data and associated service data to data recipients.

In order to fulfil their obligations, companies conclude contracts. According to the legislator, they should act autonomously in principle.[385] In order to ensure fair contractual conditions with regard to mandatory data access and to prevent the exploitation of any existing market power by one of the contracting parties, the legislator considered a provision necessary to prevent the realisation of the aforementioned risks.[386] Art. 13 DA can therefore be understood as a comprehensive clause control for B2B contracts. In this respect, the provisions of Art. 3 to 12 DA refer to the clause control of Art. 13 DA.[387]

The wording and structure of the clause control are based on various existing regulations: For example, the similarity to Annex 1 Chapter 8 of the failed proposal for the Common European Sales Law (CESG) has already been noted in the literature.[388] In addition, parallels to the Late Payment Directive[389] are obvious, even though Art. 13 DA only contains the instrument of clause control and does not address detrimental commercial practices in general or the lack of transparency of contractual terms.[390] Others see Art. 13 DA as largely modelled on Directive 93/13/EEC[391] in terms of its structure and wording.[392] The latter is noteworthy insofar as Directive 93/13/EEC had a considerable influence on the standards of German law on general terms and conditions.[393] Due to the similar regulatory structure, it could therefore be considered to transfer large parts of the dogmatics and case law on Directive 93/13/EEC to Art. 13 DA, taking into account the restriction that Directive 93/13/EEC only applies to B2C relationships, while Art. 13(1) DA only applies to B2B relationships.[394]

b) Scope of the clause control: B2B contracts

Art. 13(1) DA determines, on the one hand, the legal consequences in the event of the use of unfair contractual terms and, on the other hand, the scope of the clause control: According to this, contractual clauses relating to data access and use or liability and remedies for breach or termination of data-related obligations unilaterally imposed by **one company** on **another company** are not binding on the latter if they are unfair. The provision is not at the disposal of the contracting parties (Art. 13(9) DA). In contrast

385 Rec. 59 Regulation (EU) 2023/2854.
386 Rec. 44 Regulation (EU) 2023/2854; to avoid gatekeeper effects, see Rec. 58 Regulation (EU) 2023/2854.
387 See Art. 8 (1)(2) DA.
388 Staudenmayer, D., *NJW* 2024, 1377 (1378); Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law, COM (2011) 635.
389 Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions, OJ L 48, 23.2.2011, p. 1 et seq.
390 See Art. 7 and Art. 8 Directive 2011/7/EU; Schwamberger, S., *MMR* 2024, 96; v. Westphalen, F., *BB* 2024, 515.
391 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29 et seqq.
392 Lettl, T., *WM* 2024, 185; Schwamberger, S., *MMR* 2024, 96.
393 MüKO BGB/Fornasier, M., Vor. § 305 para. 23.
394 Lettl, T., *WM* 2024, 185; more details in section 4.d.

to the first Commission draft of the Data Act, micro-enterprises and SMEs are not privileged.[395] There it was still stated that the abuse control was only applicable if the party affected by the clause was a micro-enterprise or SME, so that larger companies could not have invoked their advantages.[396] This differentiation no longer exists.

In addition to the B2B context, Art. 13(1) DA stipulates two further requirements that must be met cumulatively. These are (aa) contractual clauses relating to data access and use or liability and remedies for breach or termination of data-related obligations that (bb) one company **unilaterally imposes** on the other company.

aa) Contractual clauses relating to data access and use or liability and remedies for breach or termination of data-related obligations

The first requirement is an expression of the idea that the clause control should only apply to those parts of a contract that relate to the provision of data.[397] In practice, this can lead to a "**split review of content**".[398] Accordingly, the provisions of Art. 13 DA would apply to some clauses of a contract, while general GTC law would have to be used for other clauses. Furthermore, the contractual clauses do not have to be pre-formulated for a large number of contracts.[399]

The first requirement refers to the already mentioned reference to Art. 3 to 12 DA, which regulate data access and data use claims in more detail. Art. 8(1) and (2) DA declares Art. 13 DA to be directly applicable to these chapters, in particular to Art. 5 DA. The exact relationship between the control under Art. 13 DA and the **FRAND conditions** defined in Art. 8(1) DA is doubtful. It is argued that in such cases, Art. 13 DA should apply as a differentiation of the FRAND conditions, irrespective of whether a clause is unilaterally imposed.[400] However, this view fails to recognise that, according to the wording, the scope should only apply to unilaterally imposed clauses.[401] If, on the other hand, the general applicability of Art. 13 DA to Art. 3 to 12 DA were to be rejected, only a very limited scope would remain.

The question of whether the switching of data processing services under Art. 23 DA can also be regarded as data access or use is also problematic. In some cases, it has been suggested that the evaluations of Art. 13 DA should be taken as a basis in order to characterise the inappropriateness of a "switching fee" in more detail.[402] However, the answer to this question is largely irrelevant, as contractual clauses relating to liability and remedies in the event of a breach or termination of data-related obligations pursuant

395 Rec. 45 Regulation (EU) 2023/2854; v. Westphalen, F., *BB* 2024, 515.
396 See Art. 13(1) COM(2022) 68 final.
397 Rec. 60 Regulation (EU) 2023/2854.
398 Wiebe, A., *GRUR* 2023, 1569 (1574).
399 Jung, S., *ZIP* 2024, 1565 (1567).
400 With reference to the system of Art. 8(2) DA Schwamberger, S., MMR 2024, 96, 97; Drexl, J., et al., Position Statement, para. 128 et seq.
401 Rec. 59 Regulation (EU) 2023/2854; finally, the decisive factor is whether Art. 8(2) DA should constitute a partial or complete reference to a legal basis. For more details, see also Chapter A. I. 4. d) bb) (2) (a).
402 v. Westphalen, F., *BB* 2024, 515 (521).

to Art. 13(1) DA are also subject to clause control under this article; the provisions on data processing services in Art. 23 et seq. DA undoubtedly contain data-related obligations.

bb) Imposed unilaterally

The second requirement of Art. 13(1) DA concerns the unilateral imposition by a company. According to Art. 13(6) DA, a contractual clause is deemed to be unilaterally imposed if it is introduced by a contracting party and the other contracting party cannot influence its content despite attempting to negotiate it.

If one asks about the purpose of this regulation, one can refer back to what has already been said about the position of dominant companies.[403] If companies are under a legal obligation to co-operate or in cases where new or small companies are seeking to participate in a market, in many situations they will have to give their consent to conditions that they would not have agreed to as an equal partner. The legislator obviously had so-called "***take-it-or-leave-it*** situations"[404] in mind when drafting Art. 13 DA, as is made clear in recital 59. This refers to

> Situations without room for negotiation where one party introduces a specific contractual term and the other company cannot influence the content of this term despite attempts to negotiate. Contractual clauses that are only introduced by one party and accepted by the other company, or clauses that are negotiated between the parties and subsequently agreed in a modified form, should not be considered unilaterally imposed.

(1) Requirement of a negotiation attempt?

This principle is also reflected in Art. 13(6) DA. However, the scope of the clause control is considerably limited by the restriction to such situations: Accordingly, the company on which the clause was imposed must at least **attempt to negotiate** to amend the relevant clause. In this respect, it is not important whether the user was actually subjectively prepared to enter into negotiations.[405] Rather, the decisive factor is whether, from an objective point of view, attempts at negotiation have taken place. The user party cannot invoke the unfairness of the term, Art. 13(6) DA. Furthermore, the party who introduced the clause has the burden of proof that the clause was not introduced unilaterally, Art. 13(6) DA. The negative wording could be an indication of a legal presumption to the effect that introduced clauses are generally considered to be unilaterally imposed.

In practice, the requirement of an attempt to negotiate could have the effect that a formal attempt is made to open up the scope of clause control. This approach harbours the risk that less experienced contracting parties introduce clauses and more experienced contracting parties feign attempts to negotiate in order to subsequently subject the contract to clause control in their favour through legal action, which would

403 See also Rec. 58 Regulation (EU) 2023/2854.
404 Rec. 59 Regulation (EU) 2023/2854; Wiebe, A., *GRUR* 2023, 1569 (1574).
405 Beinke, L./Daute, I., *RDi* 2024 (70).

run counter to the intended protection of new entrants to the market.[406] If, on the other hand, the introducing party wishes to avoid clause control, it is argued that the inclusion of a simple ***accept button*** is appropriate, with the result that no attempt at negotiation can take place.[407] This view is based on the wording of recital 59, which states that contractual clauses which are *accepted* by the other company are not deemed to be unilaterally imposed.[408] The wording "accept" is therefore interpreted as an externally perceptible act. If, on the other hand, a subjective component is emphasised, according to which acceptance presupposes an actual, internal agreement, it could be argued in the sense of a first-right conclusion that the person who is merely offered an *accept button* is more worthy of protection than the person who was even able to attempt to negotiate. Such an understanding is supported not least by the fact that the legislator's aim was precisely to cover *take-it-or-leave-it* situations through Art. 13 DA.[409] In addition, this also prevents the exploitation of dominant market positions to an even greater extent.[410]

Finally, the question arises as to whether an attempt to negotiate must be made for each individual clause or whether an attempt to negotiate a single clause is sufficient. The plural wording of Art. 13(6) DA ("contractual clauses") is in favour of this.[411] However, in view of the wording formulated in the singular in other language versions, this must be a translation error.[412] The narrow understanding of recital 59 also speaks in favour of this.[413] An attempt at negotiation must therefore be made for each clause for the applicability of Art. 13 DA.

(2) Statement

According to the view expressed here, it follows from Art. 13(6) DA that contractual clauses can only be regarded as unilaterally imposed within the meaning of the standard if the other contracting party has previously attempted to negotiate. When an attempt at negotiation has been made must be determined on the basis of objective circumstances. The subjective willingness of the other contracting party to negotiate is at most of indicative significance. This assessment is necessary in view of the clear wording of Art. 13(6) DA, even if the legislator thereby severely limits the scope of Art. 13 DA and the objective pursued of strengthening new entrants in negotiations with market-dominant companies is at least partially missed. The performance or non-performance of a negotiation attempt can thus serve as an instrument for one or both parties to circumvent the clause control at will. Attempts to negotiate must be made for each clause; an attempt to negotiate a single clause is not sufficient.

406 Wiebe, A., *GRUR* 2023, 1569 (1575); Rec. 58 Regulation (EU) 2023/2854.
407 Wiebe, A., *GRUR* 2023, 1569 (1575).
408 In the English version of the DA, the wording "accept" is used.
409 See wording of Rec. 59 Regulation (EU) 2023/2854 (English version).
410 Rec. 58 Regulation (EU) 2023/2854.
411 Jung, S., *ZIP* 2024, 1565 (1568).
412 In English: "A contractual term"; In French: "Une clause contractuelle"; In Spanish: "una clásula contractual"; Jung, S., *ZIP* 2024, 1565 (1568) et seq.
413 Jung, S., *ZIP* 2024, 1565, (1568).

The use of *accept buttons* means that no attempts at negotiation have been made and the clauses are not to be regarded as unilaterally imposed. Rather, accept buttons regularly represent *take-it-or-leave-it* situations, which Art. 13 DA, according to the recitals, aims to prevent.

In terms of time, the provisions of Art. 13 DA apply to all contracts concluded after 12 September 2025 in accordance with Art. 50 DA. In addition, according to Art. 50 DA, Art. 13 DA applies to contracts concluded on or before 12 September 2025 from 12 September 2027, provided that they are of indefinite duration (a) or their term of validity ends at the earliest 10 years after 11 January 2024 (b).

cc) Relationship to the control of general terms and conditions under national law, Art. 1(9) DA

In addition to the control of unfair contract terms for B2B contracts on data access and data use in accordance with Art. 13 DA, there is a general control of general terms and conditions in the national law of the member states, which goes back to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. The aim of the directive was to establish uniform minimum standards in the European Union to protect consumers from unfair contract terms. It obliges the member states to create regulations that declare unfair terms in contracts between companies and consumers invalid.

The question arises as to the relationship between the national provisions on the control of general terms and conditions and Art. 13 DA. According to Art. 1(9) DA, the provisions are merely supplemented by the Data Act and remain otherwise unaffected. While Directive 93/13/EEC only lays down requirements for the B2C relationship, Art. 13 DA only applies in the B2B area (Art. 13(1) DA). Therefore, direct overlaps between the two legal acts are initially excluded.

German law is characterised by the fact that the national legislator has transposed Directive 93/13/EEC excessively and extended the scope of the control of general terms and conditions in § 305 et seq. BGB to B2B relationships.[414] This actually raises the question raised above about the relationship between § 305 et seq. BGB to Art. 13 DA. The differentiation already mentioned in view of the data-relatedness is continued by the characteristic of unilateral imposition. However, if it is a unilaterally imposed clause with data reference, the relationship to German GTC law is problematic. The distinction becomes particularly virulent with regard to the different evaluations and legal consequences of both regulatory regimes in the event of an unfair term, as the following example illustrates: A term that excludes liability for breaches of duty caused by (simple) negligence in a data-related duty context would be considered an unreasonable disadvantage within the meaning of § 307(2) No. 2 BGB and would therefore be invalid.[415] In contrast, the same clause would be compatible with Art. 13 DA because Art. 13(4)(a) DA only

414 Riesenhuber, K./Habersack, M./Mayer, H.C., Europäische Methodenlehre, § 14 (46); v. Westphalen, F./Thüsing, G./ Pamp, J./Thüsing, G., Vertragsrecht und AGB-Klauselwerke, 50th EL 2024, Part: Klauselwerke, Europäische Grundlagen des AGB-Rechts, (103).

415 Beinke, L./Daute, I., *RDi* 2024, 69 (71).

prohibits the exclusion of liability for intentional and grossly negligent acts or categorises them as abusive. The Data Act does not contain any provisions for such a collision case with deviating results, meaning that the outcome would remain open until clarified by case law.[416] In the event of the scope of § 305 et seq. BGB and Art. 13 DA, which is likely to be the case in many constellations due to the similar requirements, the question of the competing relationship arises. In the absence of an explicit provision in the Data Act, recourse could be made to the primacy of Union law, whereby it could be problematic in detail how far the primacy of the Data Act extends compared to German law on general terms and conditions.[417] In addition, the question arises as to whether national provisions can concretise European regulations without an opening clause; this has always been controversial.[418] If the answer is no, this means that in some member states, which previously had no T&C control in the B2B area, this is now possible for the first time, even if only in the area of data-related use, while in other member states, such as Germany, an existing system is broken up by an area exception.[419] Ultimately, this question will have to be clarified by the ECJ.

c) Abuse control

In the instance that the scope is deemed to be open, the question of whether the content of the clause is considered to be unfair in detail arises. Art. 13(2) and (8) DA exempt clauses with certain contents from abuse control. This is initially plausible for clauses in which *essentialia negotii* of the contract (Art. 13(8) DA) are defined. Accordingly, the appropriateness of the price in particular is not subject to review on the basis of Art. 13 DA. Conversely, only clauses relating to ancillary contractual obligations fall within the scope of Art. 13 DA. The categorisation of Art. 13(2) DA is more difficult, according to which contractual clauses that comply with mandatory provisions of Union law (first alternative) or, in the absence of contractual clauses regulating the matter, applicable provisions of Union law (second alternative), are not considered unfair. At first glance, it is difficult to determine the content of the second alternative. The English translation of the text of the standard provides insight into the matter: It can thus be concluded that the terms in question are not to be considered as unfair on the basis that they (1.) are in compliance with the mandatory provisions of Union law or (2.) merely reproduce the provisions of Union law; that is to say, they are of a purely declaratory nature.[420] This means that only provisions for which Union law makes no stipulations and those that represent deviations from mandatory Union law, but not the mandatory law itself, can be reviewed.[421]If a term fulfils these requirements, Art. 13(3) – (5) DA sets out standards by which the unfairness of the terms is to be assessed. The regulatory structure is similar to the provisions in German law, namely §§ 307–309 BGB, with the special feature that,

---

416 Beinke, L./Daute, I., *RDi* 2024, 69 (71); Art. 13(4)(b) DA only concerns liability for the non-fulfilment of contractual obligations, but not for poor fulfilment.
417 Beinke, L./Daute, I., *RDi* 2024, 69 (71) et seq.
418 Schmidt-Kessel, M., *JZ* 1998, 1135 (1136) et seq.; Beinke, L./Daute, I., *RDi* 2024, 69 (71) et seq.
419 Beinke, L./Daute, I., *RDi* 2024, 69 (72).
420 Schwamberger, S., *MMR* 2024, 96 (98).
421 Schwamberger, S., *MMR* 2024, 96 (98).

unlike in the BGB, the specific prohibitions on terms also apply in B2B relationships. The system of abuse control is as follows: Art. 13(3) DA contains a **general clause** as to when a contractual term should be considered unfair. Art. 13(4)(a) –(c) DA lists a non-exhaustive ("in particular") catalogue of various terms without evaluation options ("**black list**").[422] Art. 13(5)(a)–(g) DA, on the other hand, contains a catalogue of various clauses with the possibility of evaluation, the existence of which is presumed to be unfair ("**grey list**").[423]The system of abuse control and the principle of speciality[424] determine the order in which the clauses are reviewed: First, the contractual clauses in question must be examined for their compatibility with the special requirements of Art. 13(5)(a)–(g) DA, followed by the catalogue of clauses with evaluation options in accordance with Art. 13(4)(a)–(c) DA. If the clause does not violate either Art. 13(5) DA or (4), the clause must be checked for compatibility with the (subsidiary) general clause of Art. 13(3) DA.

aa) "Blacklist" (Art. 13(4) (a)–(c))

According to Art. 13(4) DA, a contractual term is considered unfair in particular if it has the purpose or effect of excluding liability for grossly negligent breaches of duty by a party (a).[425] The same applies to clauses that have the purpose or effect of excluding the legal defence options of the party on whom the clause is imposed or excluding liability for breaches of duty by the imposing party (b).[426]

Furthermore, Art. 13(4) DA applies to such clauses which have the purpose or effect that the imposing party has the possibility to determine whether the data provided is in accordance with the contract and thus unilaterally enable it to interpret the contract (c).[427]

bb) "Grey list" (Art. 13(5)(a) – (g) DA)

According to Art. 13(5) DA, a term is considered unfair if it unreasonably limits the remedies of the party on whom the term is imposed or the liability of the imposing party in the event of non-performance or poor performance or extends the liability of the former party (a).[428]

The aforementioned assertion is equally applicable if the clause contains access rights for the imposing party and this significantly harms the party on which the clause is imposed, in particular through access to business secrets (b),[429] and if the company that provides the data and on which the clause was imposed is prevented or unreasonably hindered from accessing or using its data (c).[430]

---

422 Schwamberger, S., *MMR* 2024, 96 (99).; Staudenmayer, D., *NJW* 2024, 1377 (1380).

423 Here, too, the classification of whether or not there are valuation options is not readily apparent from the text of the standard ("in particular"), but from Rec. 62 Regulation (EU) 2023/2854; v. Westphalen, F., *BB* 2024, 515 (516); Schwamberger, S., *MMR* 2024, 96 (98) et seq.; Etzkorn, P., *RDi* 2024, 116 (122).

424 On the principle of speciality Riesenhuber, K., Europäische Methodenlehre, § 10 (31).

425 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 44 et seq.

426 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 48 et seq.

427 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 50 et seq.

428 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 54 et seq.

429 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 57 et seq.

430 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 61.

This also applies if the party is prevented from terminating the contract within a reasonable period of time (d)[431] or if the party is prevented from obtaining a copy of the data provided by it during the term of the contract or within a reasonable period of time after termination (e).[432] In addition, the granting of an unreasonably short notice period by the imposing party with the associated consequences without serious grounds (f) is covered.[433]

A unilateral right to amend the contract with regard to certain contents of the contract (g) is also included, but not if the imposing party sets out in the contract, stating valid reasons, why a unilateral right to amend the contract is required and the other party is notified of intended amendments with a reasonable period of notice and is entitled to a right of termination free of charge in such a case, Art. 13(5) DA.[434]

The contractual clause in question must have as its *object* or *effect* the content of the aforementioned prohibitions, Art. 13(5) DA. The wording suggests that it is not the intention of the party imposing the clause that is important, but only an objective consideration of the clauses. It is also irrelevant whether the clause has actually impaired the other party to the contract. Overall, this makes it easier for the party on whom the clause was imposed, as it does not have to prove that the other party intended to use the clause in bad faith or that it was actually disadvantageous.

cc) General clause (Art. 13(3) DA)

If none of the clause prohibitions in Art. 13(4), (5) DA apply, the contractual clause must be examined against the general clause in Art. 13(3) DA.[435] According to this, contractual clauses are unfair if their application constitutes a gross deviation from good business practice in data access and use or violates the principle of good faith.

In contrast to German GTC law, the basic idea of the statutory provision, the transparency of the clause or the prevention of the fulfilment of the purpose of the contract are not taken into account, but rather "good commercial practices and customs."[436] It has been rightly argued in the literature that it is unclear what can be considered **good commercial practice**, or even whether such practice currently exists.[437] The latter could be questioned, in particular, in the absence of binding legal provisions on data access and use, or (at least for the time being) model contract clauses from which to derive the legislator's judgements on what is generally regarded as good business practice.[438] Recital 61 can also be used for interpretation: It states that, as a rule, terms are not unfair and that unfairness cannot be inferred solely from the fact that a term is more favourable to one party than to the other. In view of this assessment, a

431 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 62 et seq.
432 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 64.
433 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 65.
434 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 66 et seq.
435 Rec. 62 Regulation (EU) 2023/2854.
436 Witzel, M., *CR* 2022, 561 (564).
437 Witzel, M., *CR* 2022, 561 (564); Schwamberger, S., *MMR* 2024, 96 (99).
438 Schwamberger, S., *MMR* 2024, 96 (99).

deviation from good business practice appears conceivable in particular if the party on which the clause is imposed is impaired in its ability to protect its legitimate business interest in the data concerned.[439]

d) Legal consequences and enforcement

If, following the clause review, the conclusion is reached that the clause is indeed unfair, the question arises as to the resulting legal consequences. Art. 13(1) DA stipulates in this respect that unfair terms are *not* binding on the party on whom the term is imposed. This legal consequence applies by operation of law and does not require prior judicial determination.[440] As explained, only the party on whom the clause was unilaterally imposed can invoke the unfairness of a clause, but not the party introducing it, Art. 13(6) DA.

According to Art. 13(7) DA, the other contractual clauses remain effective if the unfair clause is severable from the other clauses.[441] This raises several questions. Firstly, it is unclear when a clause is to be regarded as *severable*. Based on common usage, the contract must still be able to exist in some meaningful way. The legislator was keen to preserve the validity of as many contracts as possible.[442] This interpretation is also supported by recital 62, which states that the contract **should** continue to apply in the event of the unfairness of a term, **unless** the unfair term is not severable from the other contractual terms. When exactly the contract can still exist is not clear from Art. 13 DA – in contrast to Art. 6 (1) Directive 93/13/EEC, which refers to national legislation – so that only European law provisions are to be taken into account.[443] In accordance with the case law on Art. 6 (1) of Directive 93/13/EEC, the decisive factor is therefore whether the contract, when viewed objectively, represents a balanced regulation of mutual rights and obligations according to its purpose even without the unfair term.[444] This applies in particular if the contract is still capable of fulfilment.[445] This must be assessed objectively. In particular, it is not necessary to consider whether the imposing party would otherwise not have concluded the contract or whether it would realise less profit from an economic perspective.[446]

If a clause can be separated from the other contractual clauses, the question arises as to what applies instead of the unfair clause. The Data Act does not contain any explicit provisions on this, which is why

439 Rec. 61 Regulation (EU) 2023/2854.
440 CJEU, 4 June 2009, C-243/08, para. 28 - Pannon GSM = CJEU *NJW* 2009, 2367 para. 28; Lettl, T., *WM* 2024, 185 (187).
441 Raue, B., 'DA Art. 13', in: BeckOK Datenschutzrecht, para. 75 et seq.
442 Lettl, T., *WM* 2024, 185 (188).
443 Lettl, T., *WM* 2024, 185 (188).
444 CJEU, 27 April 2023, C-705/21, para. 37 - AxFina = CJEU *WM* 2023, 1118 (37); Lettl, *WM* 2024, 185 (187) et seq.
445 Guidelines on the interpretation and application of Directive 93/13/EEC, OJ EU, 27.9.2019, C 323, p. 41; Lettl, T., *WM* 2024, 185 (188).
446 Lettl, T., *WM* 2024, 185 (188).

general provisions on the law on general terms and conditions can be used until clarification is provided.[447] In particular, it should be clarified whether purely national provisions can be used for supplementary contract interpretation. In the past, the ECJ clarified that Art. 6(1) of Directive 93/13/EEC cannot be used to close contractual loopholes by means of general national provisions.[448] The same could therefore apply to Art. 13(7) DA due to the similar wording.[449]

If, on the other hand, the clause is not severable, the reverse of Art. 13(7) DA applies, i.e. the contract as a whole is not binding on the parties. However, this could result in particular hardship for the "disadvantaged" counterparty if it wishes to adhere to the contract despite this.[450] Therefore, if it seems reasonable for him, he can, under certain circumstances, refrain from asserting the invalidity of the clause if he would be worse off if the contract did not exist than if it existed with an unfair clause.[451]

If the clause check under Art. 13 DA shows that the contractual term in question is unfair, the question arises as to whether enforcement is carried out by the disadvantaged contracting party itself ***(private enforcement)*** or, if applicable, by public authorities ***(public enforcement)***. In principle, according to Art. 37(1) DA, one or more authorities are to be designated by each Member State for the application and enforcement of the Regulation. [452] Overall, it appears doubtful whether the legislator had private enforcement of the provisions in mind when designing the Data Act.[453]

Notwithstanding this, national measures are still possible: For German law, a duty not to use unfair terms could be derived from the duty of consideration under § 241(2) BGB, for example, so that claims for damages under §s 280(1), 241(2), 311(2), (3) BGB could be considered.[454] In certain constellations, intentional immoral damage pursuant to § 826 BGB also appears conceivable.[455] Claims under § 8 UWG may also be possible for claimants under § 8(3) UWG, as the ban on unfair terms constitutes a market behaviour regulation within the meaning of § 3a UWG.[456]

e) Practical recommendations

Until the Commission adopts model contract terms pursuant to Art. 41 DA, there will therefore be a certain degree of uncertainty for companies as to what constitutes an unfair term within the meaning of Art. 13 DA. The standard contract terms will not only be helpful because they (indirectly) concretise the concept of unfairness, but also because they will be an indication of what the Commission considers to

447 For more details, see Lettl, T., *WM* 2024, 185 (188) et seq.
448 CJEU, 12 October 2023, C-645/22, para. 36 - R.A. et al. v Luminor Bank = CJEU, *WM* 2023, 2226 para. 36.
449 Lettl, T., *WM* 2024, 185 (189).
450 Lettl, T., *WM* 2024, 185 (189).
451 Lettl, T., *WM* 2024, 185 (189).
452 On the structural similarity of the governance requirements of the GDPR and the DGA Schwamberger, *MMR* 2024, 96 (99) et seq.; for more details on Art. 37 et seq. DA in Chapter I 9).
453 Schwamberger, *MMR* 2024, 96 (100).
454 Lettl, T., *WM* 2024, 185 (191).
455 Lettl, T., *WM* 2024, 185 (191).
456 Lettl, T., *WM* 2024, 185 (191).

be good commercial practice under Art. 13(3) DA.[457] Finally, from an economic point of view, model contract clauses help to reduce the transaction costs for the companies involved that arise from negotiating complex contracts.[458] Until they are published, it is advisable to use soft law instruments such as **the ALI-ELI Principles for a Data Economy**[459] or the **Default rules for data provision contracts**[460] , which are still being drafted by UNCITRAL.[461]

No recourse may be had, or only within narrow limits, to "**substitute clauses**" which, in the event of the clause being unfair, are intended to agree another clause that corresponds as far as possible to the purpose of the unfair clause.[462] **Severability clauses**, which provide for the maintenance of the remainder of the contract if a clause is to be null and void, are also inadmissible.[463] Only the provision of Art. 13(7) DA applies here. If the opposing party wishes to come within the scope of the clause control, it must attempt to negotiate; the common negotiating tactic of not negotiating in order to benefit from the GTC control cannot be used.[464]

5. Provision of data to public authorities, the Commission, the European Central Bank and Union bodies on grounds of exceptional necessity, Art. 14–22 DA

Chapter V DA regulates the provision of data to public authorities, the Commission, the European Central Bank (ECB) or a Union body on grounds of exceptional necessity.[465] For the interpretation of Art. 14 et seq. DA, recitals 63 to 77 can be consulted. In the following, the central regulations will be presented, whereby the scope will first be outlined and then the regulations on the manner of the data provision request and its fulfilment as well as the handling of the data on the recipient side will be discussed.

a) Area

The scope is largely determined by Art. 14, 15 DA. Art. 14 DA constitutes the obligation to provide data at the request of a public sector body, the Commission, the ECB or a Union body in case of exceptional necessity.

aa) Exceptional necessity of data use, Art. 15 DA

Art. 14 DA initially presupposes the **exceptional necessity** of the use of certain data for the provision of data to the designated bodies. The undefined legal concept of exceptional necessity is further specified

457 v. Westphalen, F., *BB* 2024, 515 (516).
458 In this sense also Hennemann, M./Sattler, A./König, C., Immaterialgüter und Digitalisierung, p. 90.
459 https://principlesforadataeconomy.org/the-project/the-current-draft/data-contracts/.
460 https://uncitral.un.org/en/working_groups/4/electronic_commerce.
461 Schwamberger, S., *MMR* 2024, 96 (99).
462 BGH, judgement of 26 March 2015 - VII ZR 92/14, *BGHZ* 204, 346 = *NJW* 2015, 1952; Lettl, T., *WM* 2024, 185 (188) with further evidence.
463 Lettl, T., *WM* 2024, 185 (188).
464 Jung, S., *ZIP* 2024, 1565 (1569).
465 Hereinafter also referred to as "the requesting party" or "the requesting body".

in Art. 15 DA and differentiates between two scenarios in which an exceptional necessity for the use of certain data should exist.

(1) Management of a public emergency, Art. 15(1)(a) DA

According to Art. 15(1)(a) DA, this is the case if the requested data (i.) is necessary to deal with a public emergency and (ii.) the requesting party cannot obtain this data under equivalent conditions by other means in a timely and effective manner. Both characteristics must be present cumulatively to fulfil this variant. The term "public emergency" is defined in Art. 2 No. 29 DA as

> an exceptional and temporary situation, such as public health emergencies, emergencies caused by natural disasters and major man-made disasters, including major cybersecurity incidents, which has a negative impact on the population of the Union or of a Member State or part thereof, poses a risk of serious and lasting consequences for living conditions, economic stability or financial stability, or a risk of significant and immediate damage to economic assets in the Union or in the Member State concerned, and which has been declared and officially recognised in accordance with the relevant procedures under Union or national law.

In contrast to circumstances that are planned or scheduled or that occur regularly or frequently, the temporary exceptional situation is intended to cover circumstances that are unforeseeable and limited in time.[466] The fact that in some national legal systems a state of emergency does not necessarily have to be determined and declared is problematic, which could lead to contradictions in interpretation with the constituent element.[467] The wording *or or* used in the English version of the Data Act[468] suggests that the translation of Art. 2 No. 29 DA is a translation error, meaning that the declaration or official proclamation of a state of emergency does not have to be cumulative, but is possible as an alternative.[469]

In addition, Art. 15(1)(a) DA requires that the designated organisation cannot obtain the data under equivalent conditions by other means in a timely and effective manner. According to the recitals, this should not be the case if the data is provided voluntarily by another company or can be obtained by consulting public databases.[470]

(2) Enabling the fulfilment of tasks, Art. 15(1)(b) DA

The second scenario, in which there is an exceptional necessity for the use of data, is set out in Art. 15 (1)(b) DA. According to this, an exceptional necessity may also arise outside the circumstances covered in (a) and insofar as only non-personal data are concerned, if (i.) the requesting party lacks specific data that it needs to fulfil a task assigned to it by Union or national law and if (ii.) it has exhausted all other possibilities to obtain such data in good time.

---

466 Conclusion from the concept of exceptional necessity in Rec. 63 of Regulation (EU) 2023/2854.
467 Richter, H., 'DA Art. 15', in: BeckOK Datenschutzrecht, para. 8.
468 Rec. 64 Regulation (EU) 2023/2854.
469 Richter, H., 'DA Art. 15', in: BeckOK Datenschutzrecht, para. 8.
470 Rec. 64 Regulation (EU) 2023/2854; European Commission, FAQ DA, p. 28.

From the wording ("and") it can initially be deduced that both requirements must be met cumulatively. Practical problems could arise from the fact that the requesting body must exhaust all other means available to it according to the standard, Art. 15(1)(b)(ii) DA. According to recital 65, the requesting authority must prioritise attempts to obtain the data it requires through voluntary agreements, including the acquisition of non-personal data on the market, whereby the relevant market price is offered, or through recourse to existing obligations to provide data or the adoption of new legislation that could ensure the timely availability of the data, so that a request under Chapter V DA should be the last resort.[471] This raises the question of whether the data must actually be available on the market or whether the requesting party must obtain offers from potential contractual partners.[472] It is also questionable how the **market price** is to be determined, especially if only a few companies have specific data, so that the risk of monopoly positions being exploited becomes virulent.[473] In addition, the possibility of enacting legislation to make data available could be problematic in the sense that it does not provide precise information on whether and to what extent the enacted legislation promises success, nor on whether the legislative measures must actually be initiated in order to fall within the scope of Art. 15(1)(b)(ii) DA.[474]

(3) Exemption for micro and small enterprises and exemption from the obligation to provide evidence, Art. 15(2), (3) DA

Art. 15(1)(b) DA does not apply to micro and small enterprises, Art. 15(2) DA. These are defined in more detail in Art. 2 No. 25, No. 26 DA with reference to Art. 2(2) of the Annex to Recommendation 2003/361/EC.

It is also worth noting that Art. 15(3) DA stipulates that the public sector body is not obliged to prove that it was not able to obtain the non-personal data through acquisition on the market if the specific task carried out in the public interest is the production of official statistics and the acquisition of such data is not permitted under national law. The obligation to provide evidence under Art. 15(3) DA therefore does not apply to the Commission, the ECB or other EU institutions.[475]

bb) Authorised applicants, Art. 14 DA

According to Art. 14 DA, public authorities, the Commission, the ECB or a Union body are authorised to assert a request for provision.

According to Art. 2 No. 28 DA, a public sector body is a national, regional or local authority, body or organisation governed by public law of the Member States or associations consisting of one or more of these authorities, bodies or organisations.

---

471 Richter, H., 'DA Art. 15', in: BeckOK Datenschutzrecht, para. 21.
472 Richter, H., 'DA Art. 15', in: BeckOK Datenschutzrecht, para. 22; Translated from Hennemann et al., Data Act, p. 156.
473 Richter, H., 'DA Art. 15', in: BeckOK Datenschutzrecht, para. 22; Drexl, J. et al., Position Statement para. 137; Translated from Hennemann, M., et al., Data Act, p. 156.
474 Richter, H., 'DA Art. 15', in: BeckOK Datenschutzrecht, para. 24.
475 Richter, H., 'DA Art. 15', in: BeckOK Datenschutzrecht, para. 27.

By contrast, according to Art. 2 No. 27 DA, Union bodies, offices and agencies are those bodies, offices and agencies of the Union that have been established in accordance with legal acts adopted on the basis of the TEU, the TFEU or the Treaty establishing the European Atomic Energy Community. The distinction between Member State public bodies and supranational bodies of the Union is relevant, as Art. 15 (3) DA privileges the Commission, the ECB and other bodies to a certain extent. Public undertakings under private law are excluded from the wording of Art. 2 No. 28 DA.[476] Research institutions and research funding organisations may also be established as public bodies or bodies governed by public law.[477]

cc) Obligated parties

The data holders who hold the data and who are legal entities other than public bodies are obliged to provide data, Art. 14 DA. The data holder is legally defined in Art. 2 No. 13 DA.[478] From the wording of the definition, it can be concluded that only legal persons can be data holders within the meaning of Art. 14 DA.[479] This also includes public companies.[480] However, those acting as public bodies within the meaning of Art. 2 No. 28 DA are excluded.

The data must also be held by the data holder, which conversely rules out an obligation to obtain data.[481] Finally, the question also arises as to whether data holders must be authorised to dispose of the data.[482] If the data is not held by the data holder, the data holder may refuse to provide the data in accordance with Art. 18(2)(a) DA.

dd) Further requirements

The requesting party must need the data in order to fulfil its legal duties in the public interest, Art. 14 DA. It must provide proof of this. The requirements for the proof are specified in Art. 17 DA. At the same time, the request for provision requires a duly substantiated application. The requirements for this can also be found in Art. 17 DA.

ee) Exceptions, Art. 16 DA

Art. 16 DA constitutes exceptions in which Chapter V DA should not be applicable. Art. 16(1) DA confirms the subsidiary nature of Chapter V DA in relation to existing Union or national law with regard

476 Richter, H., 'DA Art. 14', in: BeckOK Datenschutzrecht, para. 18.
477 Rec. 63 Regulation (EU) 2023/2854; Translated from Hennemann, M. et al, Data Act, p. 152.
478 See in detail under 2 d) bb).
479 Richter, H., 'DA Art. 14', in: BeckOK Datenschutzrecht, para. 16; Schröder, M., *MMR* 2024, 104 (105).
480 Rec. 63 Regulation (EU) 2023/2854; Richter, H., 'DA Art. 14', in: BeckOK Datenschutzrecht, para. 16.
481 Richter, H., 'DA Art. 14', in: BeckOK Datenschutzrecht, para. 23.
482 In favour, but without further justification: Richter, H., 'DA Art. 14', in: BeckOK Datenschutzrecht, para. 23.

to reporting, the fulfilment of requests for access to information or the proof and verification of compliance with legal obligations.[483] Furthermore, Art. 16(2) DA states that Chapter V DA is blocked for activities of the aforementioned bodies in relation to criminal offences and administrative offences.[484]

b) Requirement for data provision requests and prohibition of further use, Art. 17(1) – (3) DA

Art. 17 DA lists in (1)(a) – (j) a catalogue of substantive and formal requirements for the data provision requests pursuant to Art. 14 DA in order to make the data provision request specific, transparent and proportionate and to keep the costs and administrative burden for data holders as low as possible.[485] Art. 17(1) DA sets out substantive information obligations that the requesting party must provide to the data holder, while Art. 17(2) DA lists various other requirements.[486] The information obligations include details of the required data and metadata (a), proof of the existence of the exceptional necessity (b) and details of the purpose of the request and the intended use (c).

The requesting party may not make the data provided available for further use (Art. 17(3) DA) in order to take appropriate account of the protection of potential business secrets of the data holder.[487] Among other things, the further use of the data in accordance with the Data Governance Act (DGA) and the PSI Directive[488], Art. 17(3) DA is therefore to be excluded.[489]

The prohibition of further use does not affect the disclosure to other public authorities, the Commission, the ECB or another EU institution in order to exchange information with them regarding the circumstance pursuant to Art. 15 DA, or to disclose the data to a third party to whom the requesting party has delegated the task, Art. 17(4) DA. The data subject has the right to lodge a complaint if he or she considers that his or her rights under Chapter V have been infringed by the transfer or provision of the data, Art. 17(5) DA in conjunction with Art. 37 DA. Art. 37 DA. In addition, the Commission is to develop a model form for requests for provision that meets the requirements of Art. 17 DA, Art. 17(6) DA.

c) Fulfilment of data requests, Art. 18 DA

If a data holder receives a data access request pursuant to Art. 14 et seq. DA, it shall provide the requesting party with the data without delay, taking into account the necessary technical, organisational and legal measures, Art. 18(1) DA. According to the prevailing view, the provision does not include the

483 For more details, see Rec. 66 et seq. Regulation (EU) 2023/2854; Barczak, T., 'DA Art. 16', in: BeckOK Datenschutzrecht, para. 2 et seq.
484 Schröder, M., *MMR* 2024, 104 (105).
485 Rec. 69 Regulation (EU) 2023/2854.
486 Translated from Hennemann, M., et al, Data Act, p. 159 et seq.
487 Rec. 70 Regulation (EU) 2023/2854.
488 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56 - 83.
489 Barczak, T., 'DA Art. 17', in: BeckOK Datenschutzrecht, para. 8.

obligation to transmit the data to the requesting party, but rather merely an "**in-situ *right***".[490] This is intended to reduce the effort for the providing company.[491]

The data holder may refuse the request for provision under the conditions of Art. 18(2), (3) DA or request its amendment. According to Art. 18(2)(a) DA, he may refuse the request if he has no control over the requested data, according to Art. 18(2)(b) DA, if a similar request for the same purpose has already been made by another party and the data holder has not been informed of the deletion of the data previously provided (the requesting party is therefore required to first obtain the data from other authorised parties in accordance with Art. 17(4) DA), or in accordance with Art. 18(2)(c) DA, if the request does not meet the requirements of Art. 17(1), (2) DA. If one of these cases applies, the data holder shall, in the event of a public emergency (Art. 15(1)(a) DA), immediately and in any case within five working days of receipt of the data request and in other cases (Art. 15(1)(b) DA) immediately and in any case within 30 working days of receipt of the data request in question, refuse it or request its amendment, Art. 18(2) DA. Reasons must be given for the refusal or amendment.[492] If the data holder invokes Art. 18(2)(b) DA, he must name the public sector body or the Commission, the ECB or the Union body that previously requested data for the same purpose, Art. 18(3) DA.

Personal data must be anonymised by the data holder or, if the disclosure of personal data is necessary, at least pseudonymised, Art. 18(4) DA. In the event of divergent views of the requesting party and the data holder regarding the lawfulness of the data holder's objection, the matter shall be referred to the competent authority of the Member State in which the data holder is established in accordance with Art. 37 DA, Art. 18(5) DA.

d) Obligations in handling the data received, Art. 19 DA

If the public sector body, the Commission, the ECB or the Union body has received the data, it must comply with the provisions of Art. 19 DA when handling the data. Art. 19(1) DA stipulates that the requesting party may not use the data for any other purpose (a), must take protective measures (b) and must delete the data as soon as they are no longer required for the stated purpose and must also inform the data holder of this (c). The obligation to erase may be waived on the basis of Union and national regulations within the framework of transparency obligations (Art. 19(1)(c) DA); it may also be waived by contract.[493]

According to Art. 19(2) DA, the core area of the purpose-related duty of use also includes the fact that the data obtained may not be used to develop or improve products that compete with those of the data holder or to pass them on to a third party for this purpose. If the data to be provided includes trade secrets within the meaning of Art. 2 No. 18 DA, they must be specifically labelled as such by the trade secret

490 Translated from Hennemann, M., et al, Data Act, p. 163; Schröder, M., *MMR* 2024, 104 (106); Specht-Riemenschneider, L., *MMR* 2022, 809 (826).
491 Rec. 69 Regulation (EU) 2023/2854; Barczak, T., 'DA Art. 18', in: BeckOK Datenschutzrecht, para. 1.
492 Rec. 71 Regulation (EU) 2023/2854.
493 Rec. 73 Regulation (EU) 2023/2854.

holder – the requesting party must take appropriate and necessary measures to maintain confidentiality before disclosing the trade secrets, Art. 19(3) DA. As the benefiting party, it is responsible for the security of the data received, Art. 19(4) DA.

e) Compensation in the event of exceptional necessity, Art. 20 DA

Art. 20 DA regulates the possibility for data holders to demand compensation for the provision. According to Art. 20(1) DA, in the event of a public emergency within the meaning of Art. 15(1)(a) DA, there is no right to compensation unless the data holder is a micro or small enterprise. The reasoning behind this is that in rare cases of threats to important public goods, no compensation should be expected in principle, and that due to the exceptional nature of the situation, too great a negative impact on the data holder's business activities is unlikely.[494] Requests for provision pursuant to Art. 15(1)(b) DA occur more frequently.[495] Therefore, according to Art. 20(2) DA, the data holder is entitled to fair consideration for the provision of data, which should not be understood as payment and not as mandatory, but which should at least cover the technical and organisational costs incurred in fulfilling the request, including, where appropriate, the costs of anonymisation, pseudonymisation, aggregation and technical adaptation, and an appropriate margin.[496] At the request of the requesting body, the basis of the calculation must be provided, Art. 20(2) DA.

Art. 20(3) DA requires clarification: This does not refer solely to Art. 20(2) DA, to which micro and small enterprises are subject anyway; rather, it is to be read in conjunction with Art. 20(1) DA and is to be understood in such a way that in cases of public emergency pursuant to Art. 15(1)(a) DA, the standards on fair consideration from Art. 20(2) DA are to be applied to micro and small enterprises.[497] This is justified from the perspective of the legislator in view of the greater burden on smaller companies.[498]

No consideration is provided for the production of official statistics under the conditions of Art. 20(4) DA. If the requesting party does not agree with the amount of the consideration requested from the data holder, there is the possibility of lodging a complaint with the competent authority of the Member State in which the data holder is established, designated in accordance with Art. 37 DA, Art. 20 (5) DA.

The public sector body, the Commission, the ECB or the Union body is authorised to disclose the data if necessary for research or statistical purposes, if these are compatible with the purpose of the data request, Art. 21(1) DA.[499] The prerequisite for this is that the recipient of the data is a non-profit organisation or acts in the public interest in the sense of a task recognised under national law and is not subject to significant influence by commercial companies that could potentially gain access to the research results, Art. 21(2) DA.

494 Rec. 75 Regulation (EU) 2023/2854.
495 Rec. 75 Regulation (EU) 2023/2854.
496 Rec. 75 Regulation (EU) 2023/2854.
497 Translated from Hennemann, M., et al, Data Act, p. 168.
498 Rec. 75 Regulation (EU) 2023/2854.
499 Rec. 76 Regulation (EU) 2023/2854.

The receiving bodies must comply with the provisions on handling data pursuant to Art. 17(3) and Art. 19, Art. 21(3) DA. They may retain the data for up to six months after their erasure by the public sector body, the Commission, the ECB or the Union body, Art. 21(4) DA. If a disclosure pursuant to Art. 21(1) DA is intended, the disclosing party shall inform the data holder without undue delay, Art. 21(5) DA, and the data holder shall have the right to lodge a complaint with the competent authority of the Member State in which the data holder is established, designated pursuant to Art. 37 DA.

The wording of Article 22(1) DA merely states that the public authorities, the Commission, the ECB and the Union bodies shall cooperate with a view to implementing the provisions of Chapter V DA. However, it is also intended to provide a basis for a right to data transmission across Member States.[500] The data exchanged by way of administrative assistance may not be used improperly, Art. 22(2) DA. Art. 22(3) and (4) DA describe the procedure envisaged for the transfer.

6. Switching between data processing services, Art. 23–31 DA

a) Preliminary considerations and background to the regulation of data processing services

The Data Act contains harmonised provisions on the facilitation of **switching between data processing services** (Art. 1(1)(d) DA). These are regulated in Chapter VI DA (Art. 23 to 31 DA), which apply to all personal and non-personal data and services processed by providers of data processing services (Art. 1 (2)(e) DA). From a territorial and personal perspective, Chapter VI DA applies to **providers of data processing services** that offer such services to customers in the Union, regardless of their place of establishment (Art. 1(3)(f) DA).[501] Chapter VI DA is organised as follows:

- Removal of obstacles to an effective bill of exchange (Art. 23 DA)
- Limitation of certain obligations to the original provider (Art. 24 DA)
- Contractual clauses for the bill of exchange (Art. 25 DA)
- Information obligations for the provider of data processing services (Art. 26 DA)
- Duty to act in good faith (Art. 27 DA)
- Contractual transparency obligations (Art. 28 DA)
- Abolition of exchange fees (Art. 29 DA)
- Technical aspects of the bill of exchange (Art. 30 DA)
- Exceptions for certain data processing services (Art. 31 DA)

With its provisions, Chapter VI DA addresses the general **contractual relationship** between providers of data processing services and their customers, so that, in contrast to Chapters II and III DA, it regulates

500 See Art. 22(2) DA and Rec. 77 Regulation (EU) 2023/2854; European Commission, FAQ DA, p. 29.
501 On the market place principle, Sattler, A., *CR* 2024, 213 (215).

less the use of data or access to data.[502] Chapter VI DA therefore has a largely independent significance.[503] Nevertheless, it is embedded in the system of the Data Act in that Chapter VI DA regulates the creation of **data spaces** and the **interoperability** between them, particularly from a legal perspective.[504]

The cloud market can currently be described as an **oligopoly** dominated **by hyperscalers** such as *'Amazon Web Services', 'Microsoft Azure'* and *'Google Cloud Platform'*.[505] The purpose of this chapter is to remove those barriers that "prevent the effective implementation of switching between data processing services"[506]. Competition is to be increased and the (vendor) **lock-in effect** counteracted by creating easier exit options for customers and removing barriers to market entry for new providers.[507]

The provisions of Chapter VI DA apply to both B2B and B2C business[508] and do not differentiate between free[509] and paid offers (Art. 23(c) DA). If the user makes the switch in relation to a data processing service of the same type of service, the user should benefit from functional equivalence after the switch (Art. 23(d) DA).[510]

The background to these provisions from Chapter VI DA is that the development of rules of conduct for self-regulation under the Free Flow of Data Regulation[511] has been restrained and there is a lack of open interfaces and standards.[512] In accordance with Art. 1(7) DA, the regulation is therefore now supplemented by the minimum obligations of Chapter VI DA.[513]

---

502 Bomhard, D., *MMR* 2024, 109 (109).

503 Pommerening, P./Nickel, M., *RDi* 2024, 289 (289); Sattler, A., *CR* 2024, 213 (214).

504 Schmidt-Kessel, M., *MMR* 2024, 75 (76); see below Chapter A.8.

505 Sattler, A. *CR* 2024, 213 (213); Lagoni, J., *CR* 2024, 91 (91); Staudenmayer, D., *NJW* 2024, 1377 (1382).

506 Rec. 79 Regulation (EU) 2023/2854.

507 COM(2022) 68 final, p. 17; Bomhard, D., *GmbHR* 2022, Heft 14, R212 (R213); Bomhard, D./Merkle, M., *RDi* 2022, 168 (175); Heinzke, P., *BB* 2024, 1291 (1291); Heinzke, P., *BB* 2023, 201 (203); Karsten, L./Wienroeder, M., *RAW* 2022, 99 (105); Weinhold, R./Schröder, C., *ZD* 2024, 306 (310); Wiebe, A., *GRUR* 2023, 1569 (1576); also referred to as "provider lock-in" in Redeker, H./Bomhard, D./Siglmüller, J., Handbuch der IT-Verträge, 9.6 Data licence agreement, para. 47; Rec. 79 Regulation (EU) 2023/2854 also refers to situations of dependency.

508 Staudenmayer, D., *NJW* 2024, 1377 (1382); this also follows from the definition of customer pursuant to Art. 2 No. 30 DA, Heinzke, P., *BB* 2024, 1291 (1292).

509 This also includes the so-called cloud credits, European Commission, FAQ DA, p. 32.

510 Hennemann, M./Steinrötter, B., *NJW* 2024, 1 (5).

511 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59.

512 Rec. 79 Regulation (EU) 2023/2854, criticism of this and the possibility for companies to seek legal protection in Schmidt-Wudy, F., 'DA Art. 23', in: BeckOK Datenschutzrecht, para. 4.

513 The principle of lex posterior derogat legi priori applies. The provisions of the Free Flow of Data Regulation apply subsidiarily, Piltz, C./Zwerschke, J., *CR* 2024, 153 (154).

b) Data processing service, Art. 2 No. 8 DA

A *data processing service*[514] is a digital service[515] that is provided to a customer and enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal administrative effort or interaction by the service provider (Art. 2 No. 8 DA).[516] This definition largely corresponds to the definition of the National Institute of Standards and Technology (NIST)[517]. It is merely expanded to include the characteristics "centralised, distributed or highly distributed".

aa) Scope of the area in question

As a starting point, the definition should be understood very broadly.[518] Data processing services are a variety of services with diverse areas , functions and technical structures,[519] which are used in different areas and can vary in terms of their complexity and type of service.[520]

The DA does not restrict the scope with regard to provider size, meaning that not only the large cloud providers mentioned above, such as *'Google', 'Amazon'* and *'Microsoft'*, but also smaller service providers fall under the scope.[521] However, it would be wrong to make a blanket categorisation, as the providers can be distinguished from one another from a technical and functional perspective.[522]

The DA fills the definition with examples that include cloud and edge services.[523] The latter is noteworthy because the highly decentralised nature of data processing in **edge computing** and the predominantly centralised nature of data processing in **cloud computing** are in tension. The term data processing service is likely to regularly refer to cloud computing.[524] Whether a data processing service in the form of edge computing falls under Art. 23 et seq. DA therefore requires a precise case-by-case assessment.[525] Furthermore, online storage locations and data service providers should also be included.[526]

---

514 Also referred to as cloud services, Hennemann, M./Steinrötter, B., *NJW* 2024, 1 (1), and the providers then as cloud service providers Heinzke, P., *BB* 2024, 1291 (1291).

515 Cf. Art. 2 No. 2 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136 p. 1.

516 The term "cloud computing service", which is similar to data processing service, is defined in Art. 6 No. 30 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333 p. 80.

517 Mell/Grace, NIST Special Publication 800-145 2011, p. 2.

518 Weinhold, R./Schröder, C., *ZD* 2024, 306 (310).

519 Rec. 81 Regulation (EU) 2023/2854.

520 Rec. 87 Regulation (EU) 2023/2854.

521 Weinhold, R./Schröder, C., *ZD* 2024, 306 (308).

522 Weinhold, R./Schröder, C., *ZD* 2024, 306 (308).

523 Rec. 78 Regulation (EU) 2023/2854.

524 Staudenmayer, D., *NJW* 2024, 1377 (1382); see Art. 41 DA.

525 Pommerening, P./Nickel, M., *RDi* 2024, 289 (292).

526 Podszun, R./Pfeifer, C., *GRUR* 2022, 953 (958).

Online search engines (Art. 3(j) DSA) and online platforms (Art. 3(i)) DSA) as well as telecommunication services are also regularly not classified as data processing services due to a lack of configurability.[527]

Furthermore, services that provide content, such as video sharing platform services (§ 1 (4) No. 8 of the Digital Services Act (DDG)[528]) and online content services (Art. 2 No. 5 of Regulation (EU) 2017/1128 (Portability Regulation))[529] should not be considered data processing services.[530]

Application service provisioning and *shared hosting* are also unlikely to be data processing services, as they are not provided in an elastic or scalable manner.[531]

In contrast to the intermediaries and their data brokerage services under the Data Governance Act[532], the DA aims to include cloud providers.[533]

bb) Further characteristics of the data processing service

The legal definition of Art. 2 No. 8 DA is concretised by recital 80, which describes the other characteristics of the data processing service in more detail. Firstly, it refers to the usual categorisation based on the models for the provision of **Infrastructure-as-a-Service** (IaaS), **Platform-as-a-Service** (PaaS) and **Software-as-a-Service** (SaaS).[534] These are specially prefabricated combinations of ICT resources. Other variants such as **Storage-as-a-Service** and **Database-as-a-Service** can also be added.[535] The following characteristics are also described:

- *Computing resources* are networks, servers or other virtual or physical infrastructures, software – including software development tools –, storage, applications and services;
- *Minimal administrative effort* means that customers can allocate computing capacities such as server time or network storage space to themselves without interacting with the provider of data processing services;

527 Weinhold, R./Schröder, C., *ZD* 2024, 306 (308); a.A. Telecommunications services as digital services are data processing services, Schild, H.H., 'DA Art. 2', in: BeckOK Datenschutzrecht, para. 58.

528 The term originates from Article 1(1)(aa) Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ L 95 of 15.4.2010, last amended by Article 28 of Regulation (EU) 2024/1083.

529 Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ C 264, 20.7.2016, p.186.

530 Weinhold, R./Schröder, C., *ZD* 2024, 306 (308) et seq; Piltz, C./Zwerschke, J., *CR* 2024, 153 (154); Podszun, R./Pfeifer, C., *GRUR* 2022, 953 (958).

531 Pommerening, P./Nickel, M., *RDi* 2024, 289 (291).

532 Art. 2 No. 11 DGA.

533 Heinzke, P. *GRUR-Prax* 2023, 154.

534 Rec. 81 Regulation (EU) 2023/2854; for a more detailed description of the "as-a-Service" variants, see Mell/Grace, NIST Special Publication 800-145 2011, p. 2 f; on the distinction between PaaS and SaaS, see Heinzke, P. *BB* 2024, 1291 (1295).

535 Rec. 81 Regulation (EU) 2023/2854.

- *Location-independent* describes the provision of computing capacities via the network and access to them via mechanisms that promote the use of heterogeneous thin or thick client platforms (from web browsers to mobile devices and workstations);
- *Scalable* refers to computing resources that are flexibly allocated by the provider of data processing services, regardless of their geographical location, in order to compensate for fluctuations in demand;
- *Elastic* means computing resources that are provided and released according to demand in order to be able to quickly increase or decrease available resources depending on the workload;[536]
- *Shared pool* describes computing resources that are provided to multiple users who access the service via a common access point, but where processing is performed separately for each user, even though the service is provided via the same electronic equipment;[537]
- *Distributed* describes computing resources that are located on different networked computers or devices and that communicate and coordinate with each other by exchanging messages;
- *Highly distributed* describes data processing services where data is processed closer to where it is generated or collected, e.g. in a networked data processing device. Edge computing, a form of this highly distributed data processing, is likely to give rise to new business models and cloud services that should be open and interoperable from the outset;

In the definition of the data processing service, *ubiquitous* was translated as ubiquitous, whereas in the recitals it is translated as location-independent. Irrespective of this editorial error, the criterion should be understood as *device-independent*.[538] The criteria configurable, scalable and elastic refer primarily to the concept of **virtualisation**, which is not further defined in the DA. Virtualisation generally refers to a technology in which several operating systems or programs are run simultaneously on one computer by sharing resources such as the processor and memory. This allows different applications to run independently of each other on the same hardware as if they were running on their own computers.[539]

The main question is then whether the provision is to be understood technically or contractually and to what extent a data processing service in the value chain – for example by passing on app providers – falls outside the scope via the criterion of configurability.[540]

Of the four classic deployment models – **private cloud**, **community cloud**, **public cloud** and **hybrid cloud**[541] – the private cloud is unlikely to be categorised as a data processing service because the pool

536 The Data Act does not define whether scalability can exist indirectly in the value chain or must be provided directly by the provider. See Bomhard, D. *MMR* 2024, 109 (110).
537 This element of the offence is aimed at multi-client providers and is not excluded solely by the separate processing for each user, Bomhard, D., *MMR* 2024, 109 (110).
538 Similarly, Pommerening, P./Nickel, M., *RDi* 2024, 289 (290).
539 https://www.golem.de/specials/virtualisierung/.
540 See Rec. 91 Regulation (EU) 2023/2854.
541 Mell/Grace, NIST Special Publication 800-145 2011, p. 3.

of computing resources used is only operated for one specific customer and is therefore not shared. Finally, SaaS should only fall within the scope of the DA if the customer can configure the computing resources such as storage space, memory or processors.

c) The switching process

The switching process is of central importance for the DA's aim of facilitating exit options for customers. A basic understanding of the switching process is also a prerequisite for being able to implement the contractual requirements of Art. 25 DA.[542] This basic understanding also includes the contractual typological categorisation of switching.[543] Although the DA leaves this question open, a contract for work is to be assumed teleologically.[544]

The **switching process** results as a **three-phase model**[545] essentially from the definitions in Art. 2 No. 34 DA and Art. 23 DA and is to be contractually depicted in accordance with Art. 25 DA.[546] The three phases consist of, firstly, the request to switch and the subsequent cancellation period, secondly, the transition period for the implementation of the switch, and thirdly, a period following the switch for further data retrieval. The switch takes place between data processing services, which is why the term **cloud switching** chosen by the legislator in Art. 1(7) DA is probably to be interpreted as a drafting error, which can also be found in the English version of the DA ("cloud switching").

aa) Change, Art. 2 No. 34 DA

The starting point is the definition of **switching**, which means the process involving a source provider[547] of data processing services, a customer of a data processing service and, where applicable, an acquiring provider of data processing services, in which the **customer** of a data processing service switches from the use of one data processing service to the use of another data processing service of the same service type or another service, offered by another provider of data processing services or by an **ICT infrastructure** on its own premises, including by extracting, converting and uploading the data (Art. 2 No. 34 DA).

This allows four switching constellations to be depicted, although it is not entirely clear whether switching to another service is included:[548]

- For the same type of service to another provider;
- With the same type of service for the ICT infrastructure on your own premises;
- To another service from another provider;
- To another ICT infrastructure service on your own premises.

---

542 With reference to the Cloud T&Cs Heinzke, P., 2024, 1291 (1293) et seq.
543 Sattler, A. *CR* 2024, 213 (217).
544 Sattler, A. *CR* 2024, 213 (218).
545 Heinzke, P., *BB* 2024, 1291 (1293) et seq.
546 See below A.6.e)bb).
547 The legal definition uses a different name, but is otherwise referred to as the original provider.
548 The contradictions contained in the Data Act are described below in A.6.c)ff).

bb) Customer, Art. 2 No. 30 DA

According to Art. 2 No. 30 DA, the **customer** is a natural or legal person who has entered into a contractual relationship with a provider of data processing services in order to utilise one or more data processing services. However, the term provider is not defined.

cc) ICT infrastructure on own premises, Art. 2 No. 33 DA

The **ICT infrastructure on the customer's own premises** (so-called "insourcing"[549]) is defined in Art. 2 No. 33 DA as ICT infrastructure and computing resources that are owned, rented or leased by the customer and that are located in the customer's data centre and are operated by the customer or a third party.

dd) Same type of service, Art. 2 No. 9 DA

According to Article 2(9) DA, the **same type of service** is a set of data processing services that have the same main objective and the same service model for data processing as well as the same main functions. Recital 81 adds by way of example that while services belonging to the same type of service may have the same model for the provision of data processing services, while two databases may appear to have the same main objective, they could fall into a more detailed sub-category of comparable services after taking into account their data processing model, their distribution model and the use cases they are targeted at.

The criterion of the same service model can therefore be understood to mean that a switch from IaaS to SaaS, for example, does not fall under the scope of the same type of service.[550] Nevertheless, services of the same service type can have "different and competing characteristics such as performance, security, robustness and quality of service".[551] The aim is that the change can be made "while maintaining a minimum set of service functions".[552]

The concept of the type of service is therefore essentially determined by the service provided to the customer.[553] Despite the definition and the further explanations in the recitals, the concept of the same type of service remains in need of clarification.[554]

ee) Functional equivalence, Art. 2 No. 37 DA

The goal of achieving **functional equivalence** is closely linked to the change to the same type of service.[555] This is defined in Art. 2 No. 37 DA as the restoration – on the basis of the customer's **exportable data** and **digital assets** – of a minimum level of functionality in the environment of a new data processing service of the same service type after the switch, if the acquiring data processing service provides

549 Sattler, A., *CR* 2024, 213 (217).
550 Pommerening, P./Nickel, M., *RDi* 2024, 289 (293).
551 Rec. 81 Regulation (EU) 2023/2854.
552 Rec. 78 Regulation (EU) 2023/2854.
553 Piltz, C./Zwerschke, J. *CR* 2024, 153 (155).
554 Piltz, C./Zwerschke, J., *CR* 2024, 153 (155).
555 See Art. 23 p. 2 (d), Art. 30(1) DA and Rec. 86 Regulation (EU) 2023/2854.

a materially comparable result in response to the same input for common functions provided to the customer under the contract.

This once again demonstrates the Janus-faced nature of the provisions of the DA: on the one hand, the DA creates an obligation to achieve functional equivalence in the IaaS provision model (recital 86, Art. 30(1) DA),[556] at the same time, the DA should not oblige providers to develop new categories of data processing services in order to be able to guarantee functional equivalence.[557]

ff) Distinctions from the switching process

The **parallel use of several providers of data processing services**, as indicated in Art. 23 DA ("[...] or, where applicable, to use several providers of data processing services simultaneously"), must be distinguished from the definition of switching in Art. 2 No. 34 DA.[558] In this respect, Art. 23 sentence 1 DA contradicts the definition of switching in Art. 2 No. 34 DA. While Art. 2 No. 34 DA does not provide for parallel use, but for switching to another service or type of service, Art. 23 DA is limited to switching within the same type of service, but at the same time opens up the scope of the obligations under Art. 23 et seq. DA for parallel use. In the latter case, the purpose is already questionable because the parallel use of data processing services of the same type of service – except for reasons of (data) security – makes less sense. These divergences emphasise the "dichotomy"[559] of Chapter VI DA: In the case of parallel use of data processing services, interoperability must be ensured above all. Art. 34 DA provides for the corresponding application of selected obligations of Chapter VI DA.[560]

The deletion of exportable data and digital assets after termination of the service (Art. 25(2) (c) No. Ii and (3)(c) DA) must also be distinguished from the concept of switching. Deletion may, however, take place in the course of the transfer, as follows from Art. 25(3) DA.[561]

Finally, switching from **on-premises** to the cloud is not included in the definition of switching. On-premises refers to a model in which ICT infrastructures are operated and managed directly on site in a company instead of using external cloud services, so that the hardware and software is hosted on the company's own premises under its full control.[562] This privileging of on-premises providers is not comprehensible for either systematic reasons or teleological considerations.[563]

---

556 See also A.6.g).
557 Rec. 92 Regulation (EU) 2023/2854.
558 Parallel use is also indicated in Rec. 79 Regulation (EU) 2023/2854: "[...] to use services from multiple providers without undue burden and data transmission costs".
559 Heinzke, P., *BB* 2024, 1291.
560 See below A.7; See Rec. 99 of Regulation (EU) 2023/2854; Heinzke, P., *BB* 2024, 1291.
561 It states "[...] to implement one or more of the [...] measures".
562 https://www.gdata.de/ratgeber/was-ist-eigentlich-on-premises?srsltid=AfmBOoqQrcVMaaWV_2rwnGbxNGQ3Tx08iUVE_mNLtgaAmlLBcHiF79w9.
563 Lagoni, J., *CR* 2024, 91 (94) et seq.

gg) Object of the bill of exchange

According to Art. 23 (2)(c) DA, when switching, the customer's **exportable data** and digital assets are transferred to another provider or to an ICT infrastructure on the customer's own premises; both terms are only used in Chapter VI DA.

(1) Exportable data, Art. 2 No. 38 DA

According to Art. 2 No. 38 DA, **exportable data** is input and output data, including metadata, generated directly or indirectly through the use of the data processing service by the customer or jointly, with the exception of assets or data of a data processing service provider or third parties that are protected by intellectual property rights or constitute a trade secret.[564] In contrast, Art. 25(2)(e) DA contradictorily indicates through the wording "an exhaustive list of all categories of data [...] that may be transferred during the execution of the transfer, including at least all exportable data" that further data may also be the subject of the transfer.

According to recital 82 and Art. 30(6) DA, the term exportable data does not include data related to the integrity and security of the service where the provider [...] is exposed to cybersecurity risks in the event of export. This includes, for example, data on the security architecture of the service such as firewalls, encryption methods or authentication systems, but also access data, log data, cryptographic keys and security certificates. The exceptions should not hinder or delay the implementation of the change.[565]

(2) Digital assets, Art. 2 No. 32 DA

According to Art. 2 No. 32 DA, **digital assets** are elements in digital form – including applications – for which the customer has a right of use, irrespective of the contractual relationship with the data processing service he wishes to change. Recital 83 adds metadata related to the configuration of settings, security and the management of access and control rights, as well as other elements such as representations of virtualisation technologies, including virtual machines and containers. If the customer has a right of use independent of the contract with the provider, the digital assets can be transferred.[566] Immediately following on from this, the question arises as to whether the provider has a right of refusal with regard to the transfer or even has to execute it if the customer cannot prove the independent rights of use.[567] With regard to digital assets, providers are also not obliged under Art. 30(6) DA to disclose these to a customer or other provider if they are protected by intellectual property rights or constitute a trade secret.

564 Rec. 82 Regulation (EU) 2023/2854.
565 Rec. 82 Regulation (EU) 2023/2854.
566 Rec. 83 Regulation (EU) 2023/2854.
567 Sattler, A., *CR* 2024, 213 (217).

d) Barriers to exchange, Art. 23 DA

Pre-commercial, commercial, technical, contractual and organisational obstacles can prevent the customer from effectively switching within the meaning of Art. 23(a) – (e) DA.[568] The wording "in particular" chosen in Art. 23 DA implies a non-exhaustive catalogue of obstacles to switching, so that providers could be obliged to remove every obstacle to switching. However, the categories chosen by the legislator are very elastic, undefined legal terms that are not described in more detail by the legislator and therefore leave a lot of room for interpretation to the user. It is therefore more obvious that only the categories mentioned – pre-commercial, commercial, technical, contractual and organisational – in conjunction with the enumerative catalogue (a)–(e) represent barriers to switching that must be observed by providers.[569] The open wording of the delimitation categories is likely to lead to overlaps in content and difficult delimitation issues.

Specifically, the pre-commercial and commercial obstacles are likely to include monetary aspects such as exchange fees. Technical barriers are likely to include, in particular, issues relating to data transfer,[570] API compatibility, the use of proprietary technologies and (data) security aspects. Contractual barriers could include clauses that make cancellation more difficult or make the switching process as a whole overly complex from a legal perspective. Finally, organisational obstacles such as staff shortages or procedural aspects of planning can also hinder the switch.

e) Obligations for data processing services, Art. 23–31 DA

The broad definition of a data processing service means that a large number of providers are also affected by the obligations set out in Art. 23 et seq. DA. Art. 23 DA opens the chapter and formulates the switching process independently instead of referring to the definitions used in Art. 2 No. 34 DA.[571] In addition, Art. 23 DA refers to the obligations under Art. 25, 26, 27, 29 and 30 DA. Meanwhile, Art. 24 and 31 DA are not mentioned, as these are not obligations in the strict sense, but rather limitations of the scope of Chapter VI DA; the same applies to Art. 28 DA, which has no reference to the bill of exchange. According to Art. 24 DA, the obligations under Art. 23, 25, 29, 30 and 34 DA only apply to services, contracts or business practices offered by the original provider of the data processing service; Art. 31 DA formulates exceptions.[572]

568 For the obligations, see section 6 e).
569 Piltz, C./Zwerschke, J., *CR* 2024, 153 (155); Danyeli, G., *DSRITB* 2022, 427 (431).
570 Rec. 79 Regulation (EU) 2023/2854.
571 For the resulting inconsistencies, see above A.6.c).
572 See below A.6.h).

Third parties are only affected by the obligations of Art. 23 et seqq. DA , which only apply if they carry out the switch on behalf of the customer.[573] Depending on the stage of the switching process, the parties involved bear varying degrees of responsibility.[574]

aa) Prohibition of imposition and obligation to remove, Art. 23 p. 2 DA

Art. 23 p. 2 DA concretises Art. 23 p. 1 DA ("in particular"). Providers of data processing services may not impose any pre-commercial, commercial, technical, contractual or organisational obstacles (Art. 23 p. 2 DA).[575] At the same time, there is an obligation to remove obstacles if they prevent customers from carrying out the actions listed in (a) – (e) (Art. 23 p. 2 DA). These include

- the prevention of termination (a), with reference to the notice period[576] in Art. 25(2)(d) DA;
- the prevention of the conclusion of new contracts (b) as a clause prohibition[577];
- the prevention of data transmission (c), which is concretised by the provisions of Art. 25 and Art. 26(b) and Art. 30(5) DA and also applies in particular to free offers;
- the impediment to achieving functional equivalence (d)[578] ;
- as well as "unbundling"[579] for IaaS[580] (e).

Unbundling means the separation of a specific service from other data processing services provided,[581] insofar as this is technically feasible (Art. 23 p. 2 (e) DA).

bb) Contractual clauses for the bill of exchange, Art. 25 DA

Art. 25 DA provides for comprehensive contractual minimum content obligations for switching between data processing services.[582] The associated restriction of private autonomy is more difficult to justify in B2B business.[583] The non-binding standard contractual clauses to be drawn up by the Commission by 12 September 2025[584] (Art. 41 DA) should help with the implementation of the content obligations – they should also strengthen trust in data processing services, ensure a balanced (contractual) relationship between users and providers and increase legal certainty with regard to the conditions for switching.[585]

The customer's rights and the provider's obligations must be set out in a written contract that is made available before the contract is concluded in such a way that the customer can save and reproduce it

573 Rec. 85 Regulation (EU) 2023/2854.
574 Rec. 85 Regulation (EU) 2023/2854.
575 See above A.6.d).
576 On the longer notice period under the Commission's draft Karsten, L./Wienroeder, M., *RAW* 2022, 99 (105).
577 In parallel, Art. 25(2)(a) DA applies as a clause requirement.
578 See above A.6.c)ee).
579 Bomhard, D., *MMR* 2024, 109 (110).
580 See 6 b) below.
581 Rec. 93 Regulation (EU) 2023/2854; Bomhard, D., *MMR* 2024, 109 (110).
582 For a comparison of the standard with Art. 28(3) GDPR, Piltz, C./Zwerschke, J., *CR* 2024, 153 (156).
583 Weinhold, R./Schröder, C., *ZD* 2024, 306 (310).
584 The standard contractual clauses will be developed by a group of experts, subsequently reviewed by the Commission and published by the Commission before 12 September 2027, European Commission, FAQ DA, p. 33; Sattler, A., *CR* 2024, 213 (220) et seq. already with proposals.
585 Rec. 98, 111 Regulation (EU) 2023/2854.

(Art. 25(1) DA). The written form requirement is to be interpreted autonomously under EU law and should therefore also include the electronic form[586], whereby the use of an electronic signature is recommended in practice.[587]

The clauses are mandatory, meaning that **no deviations** from this "contractual framework"[588] are permitted.[589] In B2B contractual relationships, these clauses are subject to control in accordance with Art. 13 DA; if the contractual partner is a consumer, control in accordance with national provisions that implement the requirements of the Clauses Directive[590] may be considered.[591]

(1) Clauses on the decision to switch, Art. 25(3) DA

According to Art. 25(3) DA, the contract referred to in Art. 25(1) DA must contain clauses according to which the customer may inform the provider of data processing services of its decision to take one or more of the following measures after expiry of the maximum notice period pursuant to Art. 25(2)(d) DA:

- the change to another provider, stating the new provider, which must be carried out by the customer (a);
- the switch to an ICT infrastructure on its own premises (b);
- the deletion of the customer's exportable data and digital assets (c)

(2) Minimum content obligations, Art. 25(2) DA

In addition to the clauses required under Art. 25(3) DA, Art. 25(2) DA sets out further contractual minimum content obligations that apply irrespective of the Digital Content Directive[592]. According to the wording, these are minimum content obligations, which conversely means that providers can also include additional clauses in their contracts.

(a) Change request and transition period, Art. 25(2)(a) DA

According to Art. 25(a) DA, the contract must contain a switching clause according to which the customer can switch on request or transfer all exportable data and digital assets to an ICT infrastructure on its own premises within a transition period of no more than 30 calendar days.

---

586 The criterion of storability in particular points to the electronic form, Schmidt-Wudy, F., 'DA Art. 25', in: BeckOK Datenschutzrecht, para. 15.

587 Piltz, C./Zwerschke, J., *CR* 2024, 153 (156); a.A. Schmidt-Wudy, F., 'DA Art. 25', in: BeckOK Datenschutzrecht, para. 12.

588 Piltz, C./Zwerschke, J., *CR* 2024, 153 (156).

589 Piltz, C./Zwerschke, J., *CR* 2024, 153 (156).

590 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 095, 21.4.1993, p. 29-34.

591 Piltz, C./Zwerschke, J., *CR* 2024, 153 (156).

592 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136, 22.5.2019, p. 1 - 27.

The switching process is initiated by the customer by means of an application addressed to the original provider; this is implicit in Art. 25(4) DA, which presupposes the application for switching and is intended to inform the provider of the customer's wish to switch (hence the so-called information phase).[593]

As in Art. 4(1) DA and Art. 5(1) DA, what exactly is to be understood by the constituent element "*request"* is likely to cause difficulties for the organisation of the switching process, because it is unclear what requirements are to be placed on the request and whether any action by the customer towards the provider is sufficient in this context.[594] The wording of the standard, which does not stipulate any content requirements for the request and, in particular, does not require customer identification, speaks in favour of the latter.[595] The legislative history can also be used to support this, which speaks of an "initiation of the change of provider"[596].

Furthermore, in the absence of an explicit legal provision, the question arises as to the form in which the customer must inform the provider of their wish to switch. An exclusion of certain, customary communication channels such as email or telephone by the provider is likely to be inadmissible, particularly in view of the requirement to cooperate in good faith pursuant to Art. 27 DA.[597] With regard to the form of the request, it is advisable for the provider to select a main communication channel that documents the corresponding request (electronically) for both contracting parties.[598]

The obligation to provide support for this transitional period is further specified in Art. 25(2)(a) clauses i–iv DA: During this period, the provider shall provide the customer and third parties authorised by the customer with appropriate support for the implementation of the change (i).[599] In particular, care must be taken to ensure the continuity[600] of business operations (ii) and information must be provided on known risks (iii). Overall, a high level of (data) security should be ensured (iv). This data security should also extend to a data retrieval period that lasts at least 30 calendar days and begins after the transition period (Art. 25(2)(g) DA).

The actual switch will then take place within a transitional period, which may not exceed 30 calendar days (Art. 25(2)(a) DA). During this transitional period, the customer must continue to pay the fee.[601]

(b) Exit strategy, Art. 25(2)(b) DA

Art. 25(2)(b) DA formulates a general obligation for switching, which should be set out in a clause. The provider must support the customer's **exit strategy** and provide all relevant information for this purpose.

---

593 Rec. 85 Regulation (EU) 2023/2854; Wiebe, A., *GRUR* 2023 1569 (1576).

594 Piltz, C./Zwerschke, J., *CR* 2024, 153 (156); no cancellation is explicitly meant, Schmidt-Wudy, F., 'DA Art. 25', in: BeckOK Datenschutzrecht, para. 18.

595 See above (4) for user identification in accordance with Art. 4(5) or Art. 5(4) DA.

596 Art. 24(1)(a) COM(2022) 68 final - 2022/0047 (COD); Piltz, C./Zwerschke, J., *CR* 2024, 153 (156).

597 Piltz, C./Zwerschke, J., *CR* 2024, 153 (157).

598 Piltz, C./Zwerschke, J., *CR* 2024, 153 (157).

599 Regularly found as a clause in outsourcing contracts, Schmidt-Wudy, F., 'DA Art. 25', in: BeckOK Datenschutzrecht, para. 21.

600 The continuity still described as "unrestricted" in the Commission's draft went far beyond the usual commitments in practice, see Bomhard, *GmbHR* 2022, Heft 14, R212 (R213).

601 Heinzke, P., *BB* 2024, 1291 (1294); a.A. Bomhard, D., *MMR* 2024, 109 (111).

In Art. 25(2)(e) and (f) DA, this information obligation is concretised: The provider must make an exhaustive list of all categories of data and digital assets that may be transferred during the switch, as well as those categories of data that are specific to the internal functioning of the data processing service and are excluded from the exportable data pursuant to (e) if there is a risk of breach of the provider's business secrets, provided that such exceptions do not hinder the switch pursuant to Art. 23 p. 2(c) DA.

(c) Termination of contract and notification of cancellation, Art. 25(2)(c) DA

According to Art. 25(2)(c) DA, the contract must contain a cancellation clause according to which the contract is deemed terminated and the customer must be informed of the cancellation after he has successfully changed[602] (Art. 25(2)c) DA) or the maximum cancellation period has expired (Art. 25(2)(c) DA).[603]

(d) Maximum notice period, Art. 25(2)(d) DA

The maximum cancellation period for initiating the switch may not exceed two months. The resulting lack of predictability will have a significant impact on the commercial pricing (also *revenue recognition*[604]) of providers.[605]

(e) Listing of data categories, digital assets and restriction on business secrets, Art. 25 (2)(e) and (f) DA

According to Art. 25(2)(e) DA, the contract must contain a clause stating that an exhaustive list of all categories of data and digital assets that may be transferred during the execution of the transfer, including at least all exportable data, must be listed as content. Art. 25(2)(f) DA supplements this with an exhaustive list of data categories that are specific to the internal functioning of the provider's data processing service and are excluded from the exportable data pursuant to Art. 25(2)(e) DA if there is a risk of a breach of the provider's business secrets, provided that such exceptions do not hinder or delay the transfer pursuant to Art. 23(c) DA.

(f) Minimum period for data retrieval of 30 days, Art. 25 (2)(g) DA

The contract must contain a minimum period for data retrieval of at least 30 calendar days – whereby the length is negotiable (Art. 25(2)(g) DA) – which begins after the expiry of the transition period agreed between the customer and the provider of the data processing services in accordance with Art. 25(2)(a) DA and Art. 25(4) DA.

---

602 In practice, it is probably difficult to determine or at least disputable when a change has been successfully completed, Schmidt-Wudy, F., 'DA Art. 25', in: BeckOK Datenschutzrecht, para. 36 et seq.

603 For uncertainties arising from the conceptual differences between termination and cancellation and the relationship between this and a contractual right of cancellation, see Schmidt-Wudy, F., 'DA Art. 25', in: BeckOK Datenschutzrecht, para. 33 et seq.

604 Bomhard, D./Merkle, M., *RDi* 2022, 168 (175).

605 Bomhard, D., *GmbHR* 2022, Heft 14, R212 (R213); the increase to 2 months is likely to have improved planning somewhat, see Bomhard, D./Merkle, M., *RDi* 2022, 168 (175).

(g) Deletion of the data, Art. 25(2)(h) DA

The deletion of the data must be included in the contract by means of a clause pursuant to Art. 25(2)(h) DA. All exportable data and digital assets that are generated directly by the customer or relate to the customer must be completely deleted after the end of the data retrieval period. The question here is whether this is a guarantee or assurance and to what extent the deletion process is to be technically designed.[606]

(h) Exchange fees, Art. 25(2)(i) DA

The contract must contain a clause on exchange fees (Art. 25(2)(i) DA).[607]

(3) Extension of the transitional period, Art. 25(4) and (5) DA

If the switch is not technically feasible within the 30 days, the provider must inform the customer of this within 14 days of the switch request – i.e. within the cancellation period – and can then propose an alternative transition period of a maximum of 7 months (Art. 25(4) DA). The provider must justify the technical impracticability of this. The legislator emphasises that the continuity of the service must also be guaranteed in this case.

The customer also has a right of extension (Art. 25(5) DA). However, unlike the provider, the customer can extend the transitional period to an indefinite period that it deems appropriate for its own purposes. Precisely because the customer has no explicit obligations to provide or co-operate, this right of extension could lead to a conflict.[608] In any case, this right must therefore be subject to the limits of Art. 27 DA, according to which the parties to the bill of exchange must act in good faith. Balancing the interests of both parties and taking into account Art. 25(4) DA, a maximum extension of 7 months should also be appropriate here.[609]

In addition to the question of the limitation by the provider of this far-reaching right, it is particularly unclear how Art. 25(4) and (5) DA relate to each other, whereby the wording "without prejudice" indicates an addition of the customer's right of extension. Although the contract continues to apply during the (extended) transitional period,[610] the question of remuneration during the extended transitional period arises in both cases.[611]

---

606 See Schmidt-Wudy, F., 'DA Art. 25', in: BeckOK Datenschutzrecht, para. 54 et seq.

607 See 6 f) below.

608 Sattler, A., *CR* 2024, 213 (218).

609 Schmidt-Wudy, F., 'DA Art. 25', in: BeckOK Datenschutzrecht, para. 76.

610 Rec. 87 Regulation (EU) 2023/2854.

611 During the alternative transitional period, the provider was still allowed to charge a reduced fee in accordance with Art. 24(1)(a), (2) COM(2022) 68 final; see Heinzke, P., *BB* 2023, 201 (203); Sattler, A., *CR* 2024, 213 (218), also in favour of remuneration; Bomhard, D., *MMR* 2024, 109 (111), argues in favour of no remuneration during the extended transitional period, and see Schmidt-Wudy, F., 'DA Art. 25', in: BeckOK Datenschutzrecht, para. 74, which does not contradict this.

cc) Duty to inform, Art. 26 DA

Art. 26 DA supplements the **information obligations** formulated in Art. 25 DA,[612] which only apply to customers who have either already concluded a contract or are about to conclude such a contract.[613] These information obligations go beyond the data information in Art. 25 DA and are aimed at decision-making in the context of the switching request.[614] The information is intended to eliminate knowledge deficits and support the customer's exit strategy.[615] On the one hand, an existing customer should receive information about the available procedures for switching and transfer (Art. 26(a) DA). On the other hand, the customer should be informed via a reference to an up-to-date online register of providers with details of all data structures and data formats as well as the relevant standards and open interoperability specifications (Art. 26(b) DA).[616] This online register is not to be understood as a register operated by a central body, but rather as a freely available online resource – not necessarily for the general public, but accessible via access – to which the provider can refer.[617]

dd) Cooperation in good faith, Art. 27 DA

Art. 27 DA formulates co-operation in **good** faith as a general obligation to act for *all parties involved* in the switching process and explicitly mentions the acquiring provider of data processing services. In addition, the original provider and the customer (Art. 2 No. 34 DA) are also likely to be affected by the obligation. Recital 85 extends this group of addressees to include third parties who carry out the transfer on behalf of the customer.

The obligation to cooperate in good faith is intended to ensure that the change is carried out effectively so that the data can be transferred on time and the continuity of the data processing service can be maintained. It is noteworthy that this obligation to act in good faith is known as an important principle from B2C contracts, but is rarely found in B2B contracts.[618] The undefined legal concept of *good faith* is to be interpreted autonomously under EU law[619] and can be substantiated using the criteria of the prohibition of abuse of rights, the prohibition of contradictory behaviour and the principle of proportionality.[620] It remains to be seen to what extent the practice that has already emerged to some extent in

612 Further information obligations arise from Art. 28, Art. 29(4) (see below A.6.f)bb)) and Art. 31(3) DA.
613 Heinzke, P., *BB* 2024, 1291 (1292).
614 Cf. Heinzke, P., *BB* 2024, 1291 (1292).
615 Rec. 95 Regulation (EU) 2023/2854, Heinzke, P., *BB* 2024, 1291 (1292).
616 See below A.7.
617 Heinzke, P., *BB* 2024, 1291 (1292).
618 Staudenmayer, D., *NJW* 2024, 1377 (1382).
619 Schmidt-Wudy, F., 'DA Art. 27', in: BeckOK Datenschutzrecht, para. 13; Pommerening, P./Nickel, A. *RDi* 2024, 289 (294).
620 Schmidt-Wudy, F., 'DA Art. 27', in: BeckOK Datenschutzrecht, para. 13.

case law and literature will be consolidated here and minimise the uncertainties for the parties involved.[621] Until then, Art. 8 CFR and Art. 5(1)(a) GDPR can be used comparatively for the interpretation.[622] Finally, it remains to be seen to what extent this obligation is enforceable and whether claims for damages can be asserted or fines imposed.[623]

ee) Transparency obligations, Art. 28 DA

According to Art. 28(1) DA, providers of data processing services are obliged to list on their websites the jurisdiction to which the ICT infrastructure is subject (a)[624] as well as a description of the TOMs and contractual measures that the provider has taken to prevent international state access to non-personal data or the transfer of such data (b).[625]

The websites must be listed in the contractual offer of the providers of data processing services (Art. 28(2) DA). The information must be kept up to date.[626] The effort for this is still justifiable for the designation of the place of jurisdiction, but involves considerable effort for the information from Art. 28(1)(b) DA.[627]

Art. 28 DA seems like a foreign body in Chapter VI, as the standard has no direct reference to switching between data processing services. In addition, the title of the standard is misleading because although it refers to contractual transparency obligations, the obligation is to be fulfilled vis-à-vis the general public.[628] Art. 28 DA is supplemented by Art. 32 DA.[629]

f) Gradual abolition of exchange fees, Art. 29 DA

The aim of Art. 29 DA is to gradually abolish **switching fees**. The legislator sees the levying of switching fees such as data extraction fees (Art. 2 No. 35 DA), which are not related to the actual costs of the provider, as an obstacle to efficient provider switching.[630] For this reason, switching fees are to be permanently abolished in a **two-stage process:** According to Art. 29(1) DA, providers may no longer charge switching fees – including data extraction fees, unless in the case of parallel use of several providers[631] – for the completion of switching **from 12 January 2027**; from **11 January 2024** to **12 January 2027**, providers may only charge reduced switching fees (Art. 29(2) DA). These reduced switching

621 Piltz, C./Zwerschke, J., *CR* 2024, 153 (157); comprehensively on the concept of good faith in Union law: Stempel, Treu und Glauben im Unionsprivatrecht, 2016.
622 Schmidt-Wudy, F., 'DA Art. 27', in: BeckOK Datenschutzrecht, para. 13.
623 Schmidt-Wudy, F., 'DA Art. 27', in: BeckOK Datenschutzrecht, para. 15; Bomhard, D., *MMR* 2024, 109 (111) et seq.; Pommerening, P./Nickel, A., *RDi* 2024, 289 (294).
624 This obligation is not always easy to implement if the ICT infrastructure is distributed or highly distributed (see above A.6.b)) or multiple jurisdictions arise due to the extraterritorial effect of national law such as the CLOUD Act (Heinzke, P. BB 2024, 1291, (1293)).
625 Art. 13(1)(f) GDPR and Art. 14(1)(f) GDPR apply to personal data, Heinzke, P., *BB* 2024, 1291 (1293).
626 Art. 28 (1) Hs. 2 DA; see Piltz, C./Zwerschke, J., *CR* 2024, 153 (157).
627 Piltz, C./Zwerschke, J., *CR* 2024, 153 (157).
628 Heinzke, P., *BB* 2024, 1291 (1292).
629 Heinzke, P., *BB* 2024, 1291 (1293).
630 Rec. 88 Regulation (EU) 2023/2854.
631 This is the wording of Art. 2 No. 36 DA and confirmed by the European Commission, FAQ DA, p. 31 et seq.

fees may not exceed the costs incurred by the provider in direct connection with the switching (Art. 29(3) DA). The abolition of switching fees and the proper levying of fees during the transitional period will be monitored by the Commission. To this end, Art. 29(7) DA empowers the Commission to adopt a delegated act within the meaning of Art. 45 DA.

aa) Exchange fees (Art. 2 No. 36 DA) and data extraction fees (Art. 2 No. 35 DA)

According to Art. 2 No. 36 DA, *switching charges* are charges other than standard service charges or early termination penalties levied by a provider of data processing services on a customer for the actions prescribed in the DA for switching to another provider's systems or ICT infrastructure at its own premises, including data extraction charges.[632] Recital 88 indicates that the rather vague definition is intended to cover in particular data extraction fees and costs for specific support activities of the provider during the switching process. What, in turn, is to be understood by specific support activities is left open. However, a systematic comparison with other payment obligations set out in the DA suggests that the category of specific support activities should be interpreted narrowly.[633]

For the change, the actual costs must be determined and limited to the variable costs excluding overheads.[634] A return on equity and borrowing costs can be taken into account.[635]

According to Art. 2 No. 35 DA, *data egress* charges are data transmission charges billed to customers for extracting their data via the network from the ICT infrastructure of a provider of data processing services to the systems of other providers or to ICT infrastructure on their own premises. In practice, these are often costs incurred by transporting data over the public Internet, the amount of which depends on the amount of data, the bandwidth and the geographical location.[636] Another example is the costs incurred when archived data is retrieved, as this is more expensive than accessing frequently used data connected to virtual machines.[637] Data extraction fees can still be charged under certain conditions in accordance with Art. 34(2) DA.[638]

Whether **standard service charges** are incurred[639] is likely to be regularly apparent from framework agreements or provider website information; in accordance with Art. 29(4) DA, the provider must clearly inform the potential customer of any standard service charges levied before the contract is concluded.[640] Charges for transitional services are also not switching charges, in particular because such services are

632 On the direct and potential indirect exceptions to the switching fees, see Sattler, A. *CR* 2024, 213 (219) et seq.
633 Rec. 85, 89 Regulation (EU) 2023/2854; Lagoni, J., *CR* 2024, 91 (92) with further references.
634 Schreiber, K./Pommerening, P./Schoel, P., Der neue DA, § 6 para. 65.
635 Schreiber, K./Pommerening, P./Schoel, P., Der neue DA, § 6 para. 65.
636 See the study by Hayward, A., et. al, Switching of Cloud Services Providers, 2018, section 3.1.
637 Hayward, A., et. al, Switching of Cloud Services Providers, 2018, section 3.1.
638 See item 7 c) below.
639 See also Sattler, A., *CR* 2024, 213 (219).
640 Lagoni, J., *CR* 2024, 91 (92) et seq.

provided by the customer and the provider taking over.[641] In particular, recital 85 clarifies the requirement of chargeability by stating that specialised professional transition services can also be provided by the original provider or third parties.[642] Specialised professional services other than transition and migration services do not prevent switching and can therefore be subject to charges.[643] As a result, in the absence of other examples mentioned by the legislator, data extraction fees are likely to be the main application case for switching fees within the meaning of Art. 2 No. 36 DA.[644]

Penalties charged for early cancellation are also to be regarded as switching fees (Art. 2 No. 36 DA).[645] These fees, which are better understood as cancellation fees[646] , are permitted in accordance with Art. 29(4) DA,[647] insofar as the potential customer is clearly informed of them before the contract is concluded. Whether cancellation fees may be incurred varies depending on the contract model. With the *pay-as-you-go model*, costs only arise when the service is used.[648] No cancellation fees are likely to be incurred here.[649] The *commitment model*, on the other hand, provides for a purchase obligation for a quantity of computing power.[650] In this case, the cancellation fees have the character of a penalty.[651]

bb) Duty to provide information on exchange fees, Art. 29(4)–(6) DA

According to Art. 29(4) DA, the provider must inform the potential customer of the possible fees, cancellation fees and reduced fees in accordance with (2) before the contract is concluded[652]. In addition, the customer may have to be provided with information on data processing services where switching is very complicated, costly or is impossible without significant interference with the data, digital assets or service architecture, Art. 29(5) DA.[653] This information must be published on a separate part of the provider's website or in another easily accessible manner for the customer in accordance with Art. 29(6) DA. Art. 29(6) DA specifies in this respect paras. 4 and 5 to the effect that the information must be provided in text form at the latest immediately prior to the conclusion of the contract.[654]

g) Technical aspects of the bill of exchange, Art. 30 DA

Art. 30(1) DA initially formulates the obligation to create **functional equivalence**[655] for IaaS when the user switches to a service of the same service type. The restriction to the IaaS model for this obligation

641 Lagoni, J. *CR* 2024, 91 (93).
642 Lagoni, J., *CR* 2024, 91 (93).
643 Lagoni, J., *CR* 2024, 91 (93).
644 Lagoni, J., *CR* 2024, 91 (94).
645 However, only in B2B relationships, see Sattler, A., *CR* 2024, 213 (219).
646 Lagoni, J., *CR* 2024, 91 (94); in Weinhold, R./Schröder, C., *ZD* 2024, 306 (310) "Abstandszahlung".
647 See also Rec. 89 Regulation (EU) 2023/2854.
648 Lagoni, J. *CR* 2024, 91 (94).
649 Lagoni, J., *CR* 2024, 91 (94).
650 Lagoni, J.,*CR* 2024, 91 (94).
651 Lagoni, J., *CR* 2024, 91 (94).
652 For the organisation and scope of the instruction, see Schmidt-Wudy, F., 'DA Art. 29', in: BeckOK Datenschutzrecht, para. 20.
653 Art. 29(5) DA.
654 Schmidt-Wudy, F., 'DA Art. 29', in: BeckOK Datenschutzrecht, para. 20 et seq.
655 See section 6 c) above.

results from the easier substitutability between these models compared to other as-a-service models.[656] At the same time, it remains open whether non-functional requirements such as performance can also be included under substitutability. Whether the resulting convergence of data processing services and the goal of functional equivalence are generally sensible seems doubtful, at least from a market economy perspective.[657]

The acquiring provider is primarily responsible for functional equivalence, whereby the original provider supports the change by providing appropriate information, documentation, technical support and, if necessary, the required instruments (Art. 30(1) DA).[658] The acquiring and original provider shall take their measures in accordance with Art. 27 DA (Art. 30(1) DA).

Art. 30(2) to (4) DA specifies further obligations for providers of data processing services that are not IaaS in order to implement *open innovation*.[659] Even if the scope is quite open due to the negative wording, it is likely to be PaaS and SaaS on a regular basis.[660] Providers are subject to the following obligations in particular:

- Provision of free **open interfaces** containing sufficient information about the service to enable the development of software for data portability and interoperability (2);
- ensuring compatibility with common specifications based on **open interoperability specifications** (Art. 2 No. 41 DA) or harmonised interoperability standards (3) and
- updating the online register referred to in Art. 26(b) DA in accordance with the requirements of Art. 25(3) DA (4).

In particular, the obligation to provide open interfaces free of charge should be limited for the original provider to the documentation necessary for the implementation of the open interface, as the provider is not obliged to act in the third-party infrastructure.[661]

If there are no common specifications for switching between services of the same service type or no harmonised standards for interoperability have been published, the provider shall export all exportable data in a structured, common and machine-readable format at the customer's request (Art. 30(5) DA).

Finally, Art. 30(6) DA states restrictively that providers are not obliged to develop new technologies or services as a result of the obligations described. Furthermore, digital assets that are protected by intellectual property rights or constitute a trade secret do not have to be disclosed to a customer or the other provider. Finally, providers are not obliged to compromise the security and integrity of the customer or provider.

656 Heinzke, P., *BB* 2024, 1291 (1295).
657 Heinzke, P., *BB* 2024, 1291 (1295).
658 On the provision in the Commission draft that is more unfavourable to the provider, Heinzke, P., *GRUR-Prax*, 154 (156).
659 Wiebe, A., *GRUR* 2023, 1569 (1576).
660 Heinzke, P., *BB* 2024, 1291 (1294).
661 Heinzke, P., *BB* 2024, 1291 (1295).

h) Exceptions , Art. 31 DA

Art. 31 DA conclusively formulates exceptions for certain data processing services for which selected obligations (1) or all obligations (2) should not apply. The provider must then inform the potential customer of the non-applicable obligations before concluding the contract (Art. 31(3) DA). In the absence of a corresponding provision, the criteria to be used to determine data processing services in accordance with (1) and (2) will probably be a matter for practice.[662] However, Art. 30 DA does not provide for exceptions for SMEs.[663]

aa) Individual solutions , Art. 31(1) DA

The prerequisite for the exception under Art. 31(1) DA is that most of the central functions – from a threshold of more than 50%[664] – are tailored to the specific needs of an individual customer or that all components have been developed for the purposes of an individual customer, whereby the individualisation must go beyond **customising**.[665] This can already be deduced from the criterion of configurable and a comparison with the English version of the provision (*custom-built* and *developed*). In addition, this customised solution must not be offered on a large commercial scale via the provider's catalogue of services (Art. 31(1) DA). In terms of legal consequences, Art. 31(1) DA stipulates that the obligations set out in Art. 23 (d), Art. 29 and Art. 30(1) and (3) DA, i.e. the obligations regarding functional equivalence, switching fees and interoperability, do not apply.

bb) Data processing services for testing and evaluation purposes , Art. 31(2) DA

Art. 31(2) DA formulates a further exception for data processing services that are not a full version but are provided for a limited period of time for testing and evaluation purposes. In contrast to Art. 31(1) DA, none of the obligations of Chapter VI DA should apply.

In any case, the fact that a fee is charged cannot be a decisive criterion for distinguishing the full version from data processing services for testing and evaluation purposes, as the provisions of Chapter VI DA also apply to free offers (Art. 23 p. 2 (c) DA).[666] The range of functions is also unsuitable for differentiation, as all functions may also have to be available for data processing services for testing and evaluation purposes. Whether it is a full version must therefore be determined on the basis of the circumstances of the individual case and the objective purpose of use.[667] The decisive factor here could be whether the service has already been fully developed or whether the customer still needs to be convinced of the data processing service, i.e. is still in the sales process.[668]

---

662 The exact criteria that can be used to separate commercial from individual offers will have to be seen in practice (Heinzke, P., *BB* 2024, 1291, (1296)).
663 Piltz, C./Zwerschke, J., *CR* 2024, 153 (154).
664 Thus Pommerening, P./Nickel, A., *RDi* 2024, 289 (292); a.A. 75%, BeckOK DatenschutzR/Schmidt-Wudy, DA, Art. 31(14).
665 Pommerening, P./Nickel, A., *RDi* 2024, 289 (292); Sattler, A., *CR* 2024, 213 (215) et seq.
666 Rec. 78 Regulation (EU) 2023/2854.
667 Schmidt-Wudy, F., 'DA Art. 31', in: BeckOK Datenschutzrecht, para. 21
668 Sattler, A., *CR* 2024, 213 (215).

cc) Obligation of the provider to inform about non-applicable obligations, Art. 31(3) DA

According to Art. 31(3) DA, the provider of the data processing service must inform the potential customer of the obligations that do not apply before concluding the contract. It is unclear, firstly, what the legal consequences are in the event of non-compliance with the obligation to inform and, secondly, how this obligation to inform is to be organised in concrete terms; in this respect, reference could be made to the provisions of Art. 29(4), (6) DA, although the provision does not expressly apply to Art. 31 DA.[669] In practical terms, it is likely to make a considerable difference whether the provider states that it is not subject to any obligations under Art. 29 DA or that it may – formulated positively – charge switching fees. The ratio leges should be that compliance with the standards created by the DA can be relied upon without the need for prior notification.[670] If providers deviate from these standards in the future, the customer must be informed of this for the purpose of decision-making.[671]

i) Sanctions and enforcement

It should be emphasised that non-compliance with the provisions of Chapter VI DA is not sanctioned in accordance with Art. 40(4) DA and that no fines can be imposed in accordance with Art. 83(5) GDPR. It is therefore left to the Member States to impose appropriate provisions on sanctions and to take the necessary measures for their application (Art. 40(1) DA). These sanctions must be effective, proportionate and dissuasive (Art. 40(1) DA). However, it is to be expected that the sanctioning will initially be restrained due to the higher workload of the supervisory authorities under Art. 4 et seq. DA, so that the civil law dispute is of greater importance.[672]

Civil law enforcement is carried out in accordance with Art. 39(1) DA, whereby the contract to be concluded in accordance with Art. 25 DA is subject to the civil procedural regulations of the respective member state, whereby the Brussels Ia Regulation[673] must be taken into account with regard to jurisdiction agreements.[674] In addition, the contracting parties have the right of appeal pursuant to Art. 38 DA.[675] From a competition law perspective, § 3a UWG is relevant insofar as Art. 23 et seq. DA are market behaviour regulations.[676] This means that customers may have individual claims and competitors may

669 Schmidt-Wudy, F., 'DA Art. 31', in: BeckOK Datenschutzrecht, para. 25
670 Heinzke, P., *BB* 2024, 1291 (1293).
671 Heinzke, P., *BB* 2024, 1291 (1293).
672 Piltz, C./Zwerschke, J., *CR* 2024, 153 (158).
673 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matter, OJ L 351, 20 December 2012, p. 1 - 32.
674 Piltz, C./Zwerschke, J., *CR* 2024, 153 (157) et seq.
675 In more detail Piltz, C./Zwerschke, J., *CR* 2024, 153 (158).
676 Piltz, C./Zwerschke, J., *CR* 2024, 153 (158).

have claims under competition law.[677] However, this enforcement under civil law is generally questionable, particularly in the case of provisions such as Art. 31(3) DA and Art. 27 DA.[678]

7. Unlawful government access to and unlawful government transfer of non-personal data in an international context, Art. 32 DA

a) Background and area

Art. 32 DA – similar to Art. 31 DGA[679] and Art. 62 EHDS-D[680] – aims to protect international data transfers of non-personal data from state access by third countries. This is intended to ensure that the data does not flow to third countries without appropriate safeguards.[681] In doing so, the legislator deliberately limits itself to non-personal data, as personal data is already subject to protection under Art. 41 et seq. GDPR already apply. This dichotomy can raise practical demarcation issues if, for example, it is unclear for data processing services whether the data to be transferred is also personal data.[682]

Furthermore, Art. 32 DA only covers data that is held in the Union, Art. 32(3) DA, which means that the data must be located on servers in the EU.[683] Only providers of data processing services within the meaning of Art. 2 No. 8 DA are subject to the obligation.[684] According to the wording of Art. 32 DA, the requesting party can only be a public sector body, i.e. a court or an administrative authority of a third country.[685]

Non-personal data should not be transferred without restriction, which in turn protects local markets and companies. The background to this are considerations that have already been expressed in the light of the Schrems judgements[686] with regard to data security, particularly in relation to surveillance programmes of the US intelligence services.[687] In contrast to the GDPR, which provides for a preventive ban with a reservation of authorisation for data transfer, data transfer is generally permitted under the concept of the Data Act and is only restricted by Art. 32 DA.[688]

677 Heinzke, P., *BB* 2024, 1291 (1293).
678 Bomhard, D., *MMR* 2024, 109 (110) et seq.
679 For more detailed information on the DGA, see II.
680 See COM(2022)197 final.
681 For the legal policy background to the provision, see Beyer-Katzenberger, M., 'DA Art. 32', in: BeckOK Datenschutzrecht, para. 2.
682 Beyer-Katzenberger, M., 'DA Art. 32', in: BeckOK Datenschutzrecht, para. 4.
683 Beyer-Katzenberger, M., 'DA Art. 32', in: BeckOK Datenschutzrecht, para. 5.
684 Beyer-Katzenberger, M., 'DA Art. 32', in: BeckOK Datenschutzrecht, para. 7.
685 Beyer-Katzenberger, M., 'DA Art. 32', in: BeckOK Datenschutzrecht, para. 6.
686 CJEU, 6 October 2015, C-362/14, Schrems I = CJEU *NJW* 2015, 3151; CJEU, 16 July 2020, C-311/18, Schrems II = CJEU *NJW* 2020, 2613.
687 Beyer-Katzenberger, M., 'DA Art. 32', in: BeckOK Datenschutzrecht, para. 1 et seq.
688 Translated from Hennemann, M., et al, Data Act, p. 230.

b) Duty to prevent international transfer and access by government organisations, Art. 31(1) DA

Firstly, providers of data processing services are obliged to take technical, organisational and legal measures to prevent access by a third country that is contrary to EU law or the law of the member state (Art. 32(1) DA). Such precautions serve to thwart both overt requests for data disclosure by state authorities and covert surveillance measures, whereby it is up to the obligated parties to decide which specific measures are taken.[689] There are some doubts as to whether the measures only need to relate to data access or data transfer as such, or whether only cases in which access by government agencies is prohibited are covered.[690]

c) Exceptions, Art. 31(2), (3) DA

Decisions and judgements by courts and administrative authorities from third countries only oblige the transfer of data if there is a corresponding agreement between the third country and the EU or a member state (Art. 32(2) DA). This should also include decisions by the public prosecutor's office and comparable authorities.[691]

If there is no corresponding agreement within the meaning of Art. 32(2) DA, Art. 32(3)(a) – (c) DA stipulates conditions which, if met, are permissible even in the absence of an international agreement within the meaning of Art. 31(2) DA. The requirements under Art. 31(3)(a) – (c) DA must be met cumulatively, which results from the wording "and" in (b). According to (a), the legal system of the third country from which the data request is made must be structured in such a way that the decision or judgement on which the request is based must be justified, proportionate and sufficiently specific. In addition, the addressee's reasoned objection must be examined by a competent court in the third country (b). Furthermore, the relevant legal interests of the provider under Union law or the national law of the Member State concerned must be taken into account by the third country (c).

The addressee of the decision can contact the competent national authority, which can answer whether the conditions of Art. 32(3)(a) – (c) DA are fulfilled (Art. 32(3)(2) DA).

If the data processing service is therefore obliged to transmit the data in accordance with Art. 32(2) or (3) DGA, it must be ensured that only the amount of data that is absolutely necessary is made available (data minimisation; Art. 32(4) DGA).[692] In addition, except in cases of criminal prosecution, the customer shall be informed by the data processing service that a request for access to their data has been

689 Beyer-Katzenberger, M., 'DA Art. 32', in: BeckOK Datenschutzrecht, para. 9.
690 Translated from Hennemann, M., et al, Data Act, p. 231.
691 Rec. 101 Regulation (EU) 2023/2854.
692 Beyer-Katzenberger, M., 'DA Art. 32', in: BeckOK Datenschutzrecht, para. 14.

made (Art. 32(5) DA) in order to create transparency with regard to the natural or legal persons actually affected by the request.[693]

8. Interoperability, Art. 33–36 DA

a) Overview and systematics

The provisions of Chapter VIII DA are aimed at regulating data rooms at a technical level. The provisions of Art. 33–36 DA[694] on the interoperability[695] of data spaces and data processing services as well as smart contracts thus have a significant impact on the implementation of Chapter VI DA.[696] In particular, the interoperability created by harmonised standards and common specifications for data structures and services enables the use of data in the Union.[697]

Just like Chapter VI DA[698] , the concept of interoperability is intended to promote innovation and competition.[699] Above all, the creation of interoperability prevents markets from tilting towards monopolies and enables existing monopolies to be broken up.[700]

The system of Art. 33–36 DA can be understood either as a juxtaposition[701] of the standards or as a staggered relationship in which Art. 33 DA is assumed to be the basic standard.[702] The latter cannot be inferred from the wording of the DA.[703] The understanding of the data spaces, which is not defined in the DA, is essential for the justification of a tiered system.[704] As a result, a functional interpretation that understands data spaces as "all open offers of data or data-based services on the market from the private or public sector"[705] is convincing here, so that data processing services and smart contracts can be regarded as a special case of this.

b) Interoperability of data rooms, Art. 33 DA

Art. 33 DA serves to develop interoperability standards.[706] This is based on the idea of an internal data market in which *data spaces* – such as the health data space[707] – are created.[708] The interoperability of

693 Beyer-Katzenberger, M., 'DA Art. 32', in: BeckOK Datenschutzrecht, para. 15.
694 For the system within these provisions, see Siglmüller, J., *MMR* 2024, 112 (112) et seq.
695 Defined in Art. 2 No. 40 Regulation (EU) 2023/2854, see 2 c) gg) above.
696 Siglmüller, J., *MMR* 2024, 112 (112).
697 Siglmüller, J., *MMR* 2024, 112 (112).
698 See 6 a) above.
699 Rec. 99 Regulation (EU) 2023/2854; Schreiber, K.,/Pommerening, P./Schoel, P., Der neue DA, § 7 para. 1.
700 Paal, B./Fenik, M., *ZfDR* 2023, 249 (261).
701 As indicated by the diagram in Schreiber, K.,/Pommerening, P./Schoel, P., Der neue DA, § 7 para. 2.
702 Siglmüller, J., *MMR* 2024, 112 (112) et seq.
703 Siglmüller, J., *MMR* 2024, 112 (112).
704 Siglmüller, J., *MMR* 2024, 112 (113).
705 Siglmüller, J., *MMR* 2024, 112 (113).
706 Schmidt-Kessel, M., *MMR* 2024, 75 (76).
707 See in more detail under B. II.
708 Schmidt-Kessel, M., *MMR* 2024, 75 (76).

data spaces should work towards better data access so that data can be utilised by the economy and society.[709]

aa) Participants in data rooms (1)

According to Art. 1(3)(g) DA, the DA applies to participants in data spaces. Art. 33 DA specifies the scope to the effect that participants in data spaces that offer data or data services to other participants are covered. The DA does not define what a data space is, nor who is considered a participant in such a data space. Art. 33(1) DA states that data spaces are "purpose-specific or cross-sectoral interoperable frameworks for common standards and procedures for the sharing or joint processing of data"[710].[711] In particular, data spaces are to be created in the areas of industry, mobility, health, finance, energy, agriculture and public administration.[712]

In principle, the roles of provider, recipient and intermediary can be considered as participants.[713] Providers of data or data services are covered if they offer them to other participants in data spaces.[714] This includes data holders in particular.[715] If the recipient is not also a provider of data or data services, they are not covered by Art. 33 DA. Intermediaries facilitate the transfer of data between provider and recipient.[716] Since the wording of Art. 33(1) DA also expressly refers to providers of data services, these intermediaries can be understood as participants. It should be noted, however, that against the background of the legislative history, a narrow data-related understanding must be assumed here and not every operationally supporting service is covered.[717]

bb) Essential requirements (1)

Art. 33(1)(a)–(d) DA formulates obligations in the form of essential requirements for participants in data spaces that offer data or data services to other participants. These can be divided into documentation obligations (a)–(c) – including descriptions of the data set content, licences, but also more technically detailed descriptions of the data structures and data formats – and interoperability obligations (d).[718] The DA thus focuses in particular on transparency as a principle and means of creating interoperability.[719]

In addition, the essential requirements of the European standardisation organisations (Art. 33(4) DA) or the European Commission (Art. 33(5) DA) must be taken into account in their work. If participants in data spaces implement these essential requirements, they benefit from the presumption of conformity in Art. 33(3) DA.[720]

---

709 COM(2020) 66 final, point 3.
710 Same wording as Rec. 103 Regulation (EU) 2023/2854.
711 For the possible interpretations of the data room, see Siglmüller, J., *MMR* 2024, 112 (113).
712 COM(2020) 66 final, point 5.D.
713 Otto, B., et al, Reference Architecture Model, p. 26.
714 Art. 30(1) Regulation (EU) 2023/2854.
715 Rec. 103 Regulation (EU) 2023/2854.
716 Rec. 103 Regulation (EU) 2023/2854.
717 Art. 28 (1) COM(2022) 68 final still refers to operators of data spaces.
718 Siglmüller, J., *MMR* 2024, 112 (113).
719 Schreiber, K.,/Pommerening, P./Schoel, P., Der neue DA, § 7 para. 6.
720 See section 7 b) dd) below.

cc) Concretisation through delegated acts (2)

Pursuant to Art. 45 DA, Art. 33(2) DA delegates to the Commission the power to adopt delegated acts for the further specification of the essential requirements referred to in Art. 33(1) DA.

dd) Presumption of conformity, harmonised standards, common specifications (3)–(11)

Art. 33(3)–(10) DA provides for the presumption of conformity through two alternatives. Primarily, compliance with harmonised standards that meet the requirements of Art. 33(1) DA confers a presumption of conformity (Art. 33(3) DA). Secondly, this can be done by complying with common specifications that also meet the requirements (Art. 33(8) DA). Procedures are also described as to when and how harmonised standards or common specifications are to be established.

Conformity with the requirements of Art. 33(1) DA is presumed for participants in data spaces whose data or data services comply in whole or in part with the harmonised standards – at least insofar as the requirements are covered by the harmonised standards (Art. 33(3)).

The harmonised standards that meet the essential requirements are drawn up by the European standardisation organisations mandated by the Commission (Art. 33(4) DA).

In addition, the Commission may adopt common specifications in the form of implementing acts that cover the essential requirements (Art. 33(5) DA). The following conditions apply:

- The harmonised standards were not developed or not developed on time or do not fulfil their mandate (a);
- No reference for the harmonised standards is published in the Official Journal or is not published (b).

Before preparing a draft implementing act referred to in paragraph 5, the Commission shall give notice that these conditions have been met (Art. 33(6) DA). In preparing the draft implementing act, the Commission shall take into account the advice of the EDIB and the views of other bodies or groups of experts and shall consult the relevant stakeholders (Art. 33(7) DA).

Furthermore, the conformity of the data or data services with the requirements pursuant to Art. 33(1) DA is presumed if they fully or partially comply with the common specifications and insofar as these requirements are covered by the specifications (Art. 33(8) DA).

Once a harmonised standard has been assessed by the Commission and the reference published in the Official Journal, the implementing acts corresponding to these harmonised standards are repealed (Art. 33(9) DA).

Member States may notify the Commission of the inadequacy of a common specification with regard to the Commission's requirements. Following their assessment, the implementing act may be amended (Art. 33(10) DA).

Finally, the Commission may adopt guidelines to establish interoperable frameworks for common standards and procedures for the functioning of common European data spaces (Art. 33(11) DA).

c) Interoperability for the parallel use of data processing services, Art. 34 DA

The issue of data portability is closely linked to the issue of data interoperability,[721] so that Chapter VIII DA contains provisions on the interoperability of data processing services. Art. 34 DA – as well as Art. 35(2)(a) DA – addresses the parallel use of various complementary services. These so-called multi-cloud strategies[722] are intended to stabilise operations, especially for providers of financial services in accordance with Regulation (EU) 2022/2554[723], but also to enable the planning of future-proof IT strategies and reduce dependence on individual providers.[724]

Art. 34(1) DA refers to those provisions (Art. 23, 24, 25 (2)(a) No. ii and iv, (e) and (f), Art. 30 (2) – (5) DA) that should apply accordingly to providers of data processing services in the case of parallel use. Parallel use does not include the simultaneous use of a data processing service and the ICT infrastructure on one's own premises.

Furthermore, Art. 34(2) DA provides for data extraction fees for parallel use, which will not be gradually abolished as long as these fees do not exceed the extraction costs incurred.[725]

d) Interoperability of data processing services, Art. 35 DA

The interoperability of data processing services[726] of the same type of service[727] is intended to counteract the lock-in to certain providers at the expense of competition and the development of new services.[728] Interfaces and infrastructure levels as well as software are required to create interoperability and the development of these depends on a cost-benefit analysis. [729] The ISO/IEC 19941:2017 standard is an important point of reference for Art. 35 DA.[730] Unlike Art. 33 and 36 DA, Art. 35 DA does not formulate any essential (material) requirements for interoperability, but instead sets out requirements for open interoperability specifications and harmonised standards. In addition to interoperability, Art. 35 DA also addresses (data) *portability*.

721 COM(2017) 9 final, point 5.2.
722 Also known as multi-homing in the case of parallel use, see COM(2017) 9 final, point 5.2.
723 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333/1 p. 1.
724 Rec. 99 Regulation (EU) 2023/2854.
725 On the fees, see 6 f); for a critical view in connection with the multi-cloud strategy, see Sattler, A., *CR* 2024, 213 (216); on the impact on variable actual costs and overheads, see Schreiber, K.,/Pommerening, P./Schoel, P., Der neue DA, § 7 para. 10.
726 For the term "data processing service", see 6 b) above.
727 For the term "same type of service", see 6 c) dd) above.
728 Rec. 90 Regulation (EU) 2023/2854.
729 Rec. 90 Regulation (EU) 2023/2854.
730 Rec. 90 Regulation (EU) 2023/2854.

aa) Regulatory objectives and minimum requirements (1) and (2)

Art. 35(1) and (2) DA formulates the objectives and requirements for the interoperability standards. The objectives are the interoperability between data processing services ((1)(a)), the portability of digital assets ((1)(b)), the facilitation of functional equivalence[731] ((1)(c)) and other supporting objectives ((1)(d) and (e)).

The requirements still need to be developed. It is clear from Art. 35(2) DA that interoperability is an umbrella term for interoperability in the narrower sense ((2)(a)), data portability ((2)(b)) and application portability ((2)(c)). All three refer to more specific aspects of interoperability. Interoperability in the narrower sense is to be regulated appropriately, for example with regard to transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and the interoperability of rules and specifications through open interoperability specifications and harmonised standards ((2)(a)).

bb) Creation of standards (3) – (9)

Art. 35 DA sets out two options for creating standards: open interoperability specifications and harmonised standards. The needs of SMEs must be taken into account in the standardisation process.[732]

According to Art. 35(5) DA, the Commission may, by means of implementing acts, adopt common specifications based on open interoperability specifications that fulfil the requirements of Art. 35 (1) – (3) DA. In doing so, the views of relevant authorities and other relevant bodies or expert groups shall be taken into account and all relevant stakeholders shall be consulted (Art. 35(6) DA). A Member State may inform the Commission if the requirements of Art. 35(1) and (2) DA are not met and the Commission may in turn amend the implementing act after examination (Art. 35(6) DA).

In addition, the Commission may mandate standardisation organisations to draw up harmonised standards in accordance with the requirements of Art. 35(1) and (2) DA. The wording "after consideration" and recital 100 can be understood to mean that this is a subsidiary relationship to Art. 35(3) and (5).

The common specifications and harmonised standards must be published in a central database – as a "one-stop-shop"[733] (Art. 35(8) DA). After publication, suppliers must ensure conformity with the specifications or standards within 12 months (Art. 30(3) DA).

e) Smart Contracts, Art. 36 DA

Art. 36 DA regulates *smart contracts*. According to Art. 2 No. 39 DA, these are computer programmes that are used for the automated execution of an agreement or part thereof, using a sequence of electronic records and ensuring the integrity of these records and the accuracy of their chronological order.

---

731 For the concept of functional equivalence, see section 6 c) ee) above and for the technical aspects of the bill of exchange, see 6 g) above.

732 Rec. 100 Regulation (EU) 2023/2854.

733 European Commission, FAQ DA, p. 31.

They are subject to essential requirements (Art. 36(1) DA) and undergo a conformity assessment (Art. 36(2)(f). DA) or conformity is presumed (Art. 36(4) – (11) DA). According to Art. 1(3)(g) DA, the DA applies to participants in data spaces and providers that use smart contracts and persons whose commercial, business or professional activity involves the introduction of smart contracts for others in connection with the implementation of an agreement. Although Art. 36 DA is linked to Art. 33(1)(d) DA, it can be described as a "foreign body"[734] in the DA.[735]

The applicability of the provisions of civil, contract and consumer protection law to agreements on the transfer of data from the use of smart contracts for the automated execution of such agreements remains unaffected.[736]

aa) Obliged party, application, data transfer agreement

According to Art. 36(1) DA, the provider of an application in which smart contracts are used or – in the absence thereof – the person whose commercial, business or professional activity involves the use of smart contracts for third parties in connection with the full or partial execution of a data provision agreement[737] is covered.

According to this, it is primarily the **provider of** an application that is obliged. § 1(4) No. 5 DDG, which defines the service provider as the provider of digital services, can be used to understand the term. Secondarily, in the absence of a provider, the person whose commercial, business or professional activity involves the use of smart contracts for third parties in connection with the full or partial execution of a data provision agreement is obliged.

In the context of the DA, the term "**applications**" is to be understood broadly. This includes software regardless of whether it is embedded in hardware.[738] A smart contract must be used in the application. This does not include applications that analyse smart contracts that are intended exclusively for internal use.[739]

The term "**smart** *contract*" is controversial, but the prevailing view is that it covers automated legal transactions and business processes and their documentation.[740] Examples of this include the fulfilment of contractual obligations or secondary claims.[741] Against the background of the DA, smart contracts could find their practical application in the automation of data transactions in particular.[742] In the IoT sector, smart contracts can be used, for example, when leasing a connected vehicle by triggering the

734 Siglmüller, J., *MMR* 2024, 112 (115).
735 Siglmüller, J., *MMR* 2024, 112 (115).
736 Rec. 104 Regulation (EU) 2023/2854.
737 Deviating from this, the heading of Art. 36 and Art. 36 (1)(e) DA Data Sharing Agreement states.
738 See Rec. 15 Regulation (EU) 2023/2854.
739 Rec. 104 Regulation (EU) 2023/2854.
740 Paulus, D., *JuS* 2020, 107 (107); Kaulartz, M./Heckmann, D., *CR* 2016, 618 (618); Borges, G., *CR* 2024, 425 (429); Hoeren, T./Sieber, U./Holznagel, B./Guggenberger, N., Handbuch Multimedia-Recht, Part. 13.7, para. 1; for the history of the term, see Fries, M./Paal, B./Finck, M., Smart Contracts, p. 1.
741 Paulus, D., *JuS* 2020, 107 (107).
742 Borges, G., *CR* 2024, 425 (428) et seq. in detail.

payment of the leasing instalment as soon as the car's mileage exceeds a certain limit or a certain period of time has elapsed.[743]

Smart contracts, on the other hand, are not to be understood as contracts in the legal sense – they are just a computer program and can only map a contract, but cannot be a contract themselves.[744]

Inspired by the invention of *blockchain*, smart contracts are regularly associated with this technology.[745] However, the legislator emphasises a technology-neutral understanding of the term "smart contract".[746]

The definition of a smart contract in Art. 2 No. 39 DA is to be understood in this context.

bb) Essential requirements (1)

The essential requirements for smart contracts include, in accordance with Art. 36(1)(a)–(e) DA:

- Robustness and access control mechanisms to avoid functional errors and to withstand manipulation by third parties (a) and (d);
- A "stop button"[747] , which enables the safe termination and interruption of a transaction execution (b);
- Data archiving so that the transaction data, logic and programme code of the smart contract can be archived upon termination or interruption of a smart contract (c);
- Consistency to ensure compliance with the terms of the data sharing agreement implemented with the smart contract (e).

cc) Conformity assessment (2)–(3)

The fulfilment of the essential requirements is carried out as part of a conformity assessment in accordance with Art. 36(1) DA and issued in accordance with Art. 36(2) DA.[748]

dd) Presumption of conformity (4)–(11)

The provisions of Art. 36(4)–(11) DA are almost identical in wording to those of Art. 33(4)–(10) DA, so that at this point we refer to the explanations in b)dd) is referred to here.

9. Application and enforcement, Art. 37–42 DA

Art. 37–42 DA regulate the measures for the enforcement and application of the provisions of the Data Act and define the responsibilities of the Member States, the imposition of sanctions and the role of the European Data Innovation Board (EDIB). In addition, Chapter IX standardises legal protection options

743 Oster, J., *ZfPW* 2023, 387 (389).

744 Paulus, D., *JuS* 2020, 107 (107); Kaulartz, M./Heckmann, D., *CR* 2016, 618 (621); Kipker/Birreck/Niewöhner/Schnorr, *MMR* 2020, 509 (509); Hoeren, T./Sieber, U./Holznagel, B./Guggenberger, N., Handbuch Multimedia-Recht, Part. 13.7, para. 4.

745 Paulus, D., *JuS* 2020, 107 (108); Borges, G., *CR* 2024, 425 (429); Fries, M./Paal, B./Finck, M., Smart Contracts, p. 4 et seq.

746 Rec. 104 Regulation (EU) 2023/2854.

747 Siglmüller, *MMR* 2024, 112 (115) et seq.

748 See also Rec. 105 Regulation (EU) 2023/2854 with further information according to which this conformity assessment should be carried out.

for natural and legal persons (Art. 38, 39 DA) and a mandate to the European Commission to draw up and recommend model contractual clauses for the effective implementation of the obligations established by the Data Act (Art. 41 DA).

a) Competent authorities and data coordinators, Art. 37 DA

In the area and enforcement of the Data Act, the legislator prioritises **public enforcement** by member state authorities.[749]

aa) Competent authorities, Art. 37 (1) DA

This essentially includes the establishment of competent authorities in the Member States that are authorised to apply and enforce the Data Act, Art. 37(1) DA. Member States may also designate several authorities or entrust existing authorities with the tasks and competences, Art. 37 (1) DA. The designation of the authority is not to be understood as a formal act in the sense of a notification or similar, but as the establishment of the authority under organisational law.[750] The name of the competent authority as well as its competences and powers must be communicated to the Commission, which keeps a public register of them (Art. 37(7) DA). For Germany, this task will most likely be assumed by the Federal Network Agency.[751]

Art. 37(3) DA provides (declaratory) that the supervisory authorities already responsible under the GDPR are also responsible for the protection of personal data under the Data Act. Their powers and tasks correspond to the regulations laid down in Chapters VI and VII of the GDPR. At the same time, the responsibility of specific sectoral authorities, such as for questions of data access and data use (Art. 37(4)(a) DA), remains unaffected.

bb) Tasks of the competent authorities, Art. 37(5), (8), (9), (14) DA

Art. 37(5) DA contains a catalogue of tasks and powers with which the Member States are to equip the competent authorities. These include

- promoting data literacy and raising awareness of the rights and obligations of users and organisations that fall within the scope of the Data Act (a);
- the processing of complaints about alleged violations of the provisions of the Data Act (b);
- the performance of investigations (c);
- the imposition of sanctions (d);
- the monitoring of technological and economic developments (e);
- co-operation with the competent authorities of other Member States and, where appropriate, the Commission or the EDIB (f), (g), (h);
- ensuring the abolition of exchange fees (Art. 29 DA) and

749 Translated from Hennemann, M., et al, Data Act, p. 237; Schwamberger, S., *MMR* 2024, 96 (99) et seq.
750 Roth-Isigkeit, D., 'DA Art. 37', in: BeckOK Datenschutzrecht, para. 3.
751 Remke, C., *MMR* 2024, 117 (118); Holznagel, B., *MMR* 2024, 639 (640).

- the examination of data requests pursuant to Art. 14 et seq. DA.

In contrast, the catalogue of tasks and competences here **does not** contain **any explicit power to order** the omission of violations of the provisions of the Data Act.[752] Recital 109 merely states that the sanctions to be imposed under Art. 40 DA also include warnings, reprimands or orders to bring business practices into line with the obligations laid down in this Regulation.

In addition, the competent authorities have the right to **request all necessary information** from users, data holders or data recipients in order to verify compliance with the Regulation, within the limits of the principle of proportionality in accordance with Art. 37(14) DA, whereby the request for information must always be justified.[753] This should generally be the case if the authority has sufficiently explained the circumstances of the request to the user, data holder or data recipient in writing.[754]

In the performance of their duties, the competent authorities must **not be subject to any external, direct or indirect influence**; this applies in particular to the acceptance and solicitation of instructions from other authorities or private parties (Art. 37(8) DA). Art. 37(9) DA obliges the Member States to provide the competent authorities with the necessary human and technical resources and expertise to enable them to carry out their duties effectively.

cc) Data Coordinator, Art. 37(2) DA

If several authorities are designated in the respective Member State, a **data coordinator** must also be designated *from among them* for support in accordance with Art. 37(2) DA. It remains uncertain when a data coordinator is appointed from among the authorities. With regard to Art. 37(4)(a) DA, which stipulates that the competence of the sectoral authority must be maintained in special matters of data access and data use, the legislator presumably wanted to clarify that the data coordinator cannot also be the competent authority in personal union.[755]

The tasks of the data coordinator are specified in Art. 37(6) DA: Accordingly, it serves as the central point of contact for all questions in connection with the application of the Regulation (a). Furthermore, the Data Coordinator ensures that data access requests made by public authorities due to exceptional necessity in accordance with Chapter V are made publicly available and promotes the voluntary sharing of data between public authorities and private data holders (b). In addition, the Data Coordinator must record the refusal of data access and disclosure requests and report annually to the Commission on these refusals (c). Finally, the data coordinator supports the competent authorities at their request in all tasks arising in the area of administrative cooperation, Art. 37(5) DA.

---

752 Roth-Isigkeit, D., 'DA Art. 37', in: BeckOK Datenschutzrecht, para. 12; Remke, C., *MMR* 2024, 117.
753 Rec. 107 Regulation (EU) 2023/2854.
754 Roth-Isigkeit, D., 'DA Art. 37', in: BeckOK Datenschutzrecht, para. 14.
755 Roth-Isigkeit, D., 'DA Art. 37', in: BeckOK Datenschutzrecht, para. 5; similarly Remke, C., *MMR* 2024, 117 (118).

dd) Responsibilities for legal entities, Art. 37(10) – (13) DA

In individual cases, the competent authority is always the authority in whose Member State the legal entities concerned have their establishment (**establishment principle**), Art. 37(10) GDPR, whereby in the case of seats in several Member States, the main seat is used as a basis. In order to determine the headquarters, the principles developed in accordance with Art. 4 No. 16 GDPR can be used.[756] Accordingly, the decisive factor is the registered office of the head office; the name chosen by the legal entity plays a subordinate role at best.[757]

If connected products or related services are provided or offered in the European Union and the legal entity is not established in the Union, a representative must be appointed in one of the Member States (Art. 37(11) DA), so that – in contradiction to the principle of establishment laid down in Art. 37(10) DA – the competence of the authority is based on the registered office of the representative, Art. 37(13) DA.[758] Each provider of connected products or services must appoint a representative to whom the competent authorities can turn in individual cases and who cooperates with them, Art. 37(12) DA.

ee) Administrative cooperation between Member State authorities, Art. 37(15), (16) DA

Art. 37(15) DA regulates the procedure for administrative cooperation between Member State authorities and distinguishes between assistance and enforcement measures. Both are initiated by a reasoned request from the authority, which must set out the essential background and the specific assistance requested. The authority of the requested Member State is obliged to respond to the request immediately upon receipt and to indicate what measures have been taken or are planned (Art. 37(15) DA).[759] The information exchanged and provided in this context may only be used by the authorities for the purposes of the request, Art. 37(16) DA.

b) Right to lodge a complaint, Art. 38 DA

Art. 38(1) DA provides for an individual right to lodge a complaint with the competent authorities, which is largely modelled on the right to lodge a complaint with a supervisory authority pursuant to Art. 77(1) GDPR.[760] According to Art. 38(1) DA, every natural and legal person has the right to lodge a complaint with the competent authority individually or, where appropriate, jointly with the allegation of a violation of their rights under the Data Act, Art. 38(1) DA. The data subjects must therefore provide sufficiently substantiated evidence of a breach of a subjective right conferred by the provisions of the Data Act.[761] Art. 38(1) DA does not provide any further procedural or procedural requirements, such as

---

756 Roth-Isigkeit, D., 'DA Art. 37', in: BeckOK Datenschutzrecht, para. 29.
757 Ehmann, E./Selmayr, M./Klabunde, A./Horváth, A.Z., GDPR, Art. 4 No. 16 para. 69 et seq.
758 Roth-Isigkeit, D., 'DA Art. 37', in: BeckOK Datenschutzrecht, para. 32.
759 For the element of the offence without undue delay, see BeckOK Datenschutzrecht/Roth-Isigkeit, DA, Art. 37(22).
760 Roth-Isigkeit, D., 'DA Art. 38', in: BeckOK Datenschutzrecht, para. 2.
761 Roth-Isigkeit, D., 'DA Art. 38', in: BeckOK Datenschutzrecht, para. 3.

the form of the complaint or a time limit to be observed – in this respect, in the absence of European administrative procedural law, the Member State regulations on administrative procedure are likely to apply.[762] Consequently, the VwVfG of the federal government or the federal states applies to Germany.[763] The competent authorities must process and resolve the complaints effectively and in a timely manner, Art. 38(3) DA.

aa) Possibility of private enforcement?

According to Art. 38(2) DA, the right of appeal applies *without prejudice to any other administrative or judicial remedy*. The wording chosen by the legislator raises the question of whether, in addition to public enforcement by national authorities, law enforcement by way of **private enforcement** is also permissible.

bb) Statement

One argument against this is that the legislator has not expressly provided for such legal enforcement options in the Data Act – unlike in other legal acts[764].[765] On the other hand, the legislator has largely modelled the enforcement provisions on Art. 77 et seq. GDPR.[766] In contrast to Art. 77 et seq. GDPR, however, it has not created a system of civil law enforcement provisions, as in Art. 79 et seq. GDPR, but rather deliberately decided against a similar regulation.[767]

Nevertheless, there are various reasons in favour of the admissibility of private enforcement under the Data Act: For example, it stipulates that it should not be possible for the parties to exclude the application of clause control under Art. 13 DA (Art. 13(9) DA), which would be pointless if private enforcement is rejected due to the fact that private law agreements cannot exclude administrative proceedings.[768] In addition, private law agreements on data access and use form the centrepiece of the Data Act, so that the overall conceptual structure of the Data Act also suggests private enforcement. From a systematic perspective, the possibility of private law dispute resolution set out in Art. 10 DA also speaks in favour of approving private law enforcement.[769] Finally, private enforcement before the (civil) courts of the Member States would also benefit the effectiveness of Union law (Art. 4(3) TEU). Last but not least, the open wording of Art. 38(1) DA also speaks in favour of the admissibility of private enforcement, as private enforcement is at least not expressly excluded.[770] Overall, therefore, the better arguments speak in favour of considering the enforcement of the provisions of the Data Act by way of private enforcement to be permissible.[771]

---

762 Roth-Isigkeit, D., 'DA Art. 38', in: BeckOK Datenschutzrecht, para. 4; Remke, C., *MMR* 2024, 117 (119).
763 Remke, C., *MMR* 2024, 117 (119).
764 See, for example, Art. 54 DSA; for more details, see section B.II.4.b.
765 Schwamberger, S., *MMR* 2024, 96 (100).
766 Roth-Isigkeit, D., 'DA Art. 38', in: BeckOK Datenschutzrecht, para. 2; Schwamberger, S., *MMR* 2024, 96 (100).
767 Schwamberger, S., *MMR* 2024, 96 (100).
768 Schwamberger, S., *MMR* 2024, 96 (100).
769 Remke, C., *MMR* 2024, 117 (121).
770 Schwamberger, S., *MMR* 2024, 96, 100.
771 In conclusion, Remke, C., *MMR* 2024, 117 (119); Schwamberger, S., *MMR* 2024, 96 (101), is more cautious.

c) Right to an effective judicial remedy, Art. 39 DA

In addition to other administrative or extrajudicial remedies, every person concerned has the **right to an effective judicial remedy** against legally binding decisions regarding the complaint, Art. 39(1) DA. This right also applies if the competent authority fails to take action in relation to a complaint in accordance with Art. 38(1) DA, whereby alternatively ("or") there is also the possibility of submitting the case to an impartial body with appropriate expertise (Art. 39(2) DA). The term "decision" is not defined – however, it can be assumed that not every action by an authority constitutes a decision within the meaning of the standard. Rather, the action of the authority must have a certain degree of regulatory quality for the addressee of the decision, which is likely to be lacking in the case of official investigations (Art. 37(5)(c) DA) or reports (Art. 37(5)(e) DA).[772] If a complaint is declared inadmissible or unfounded or sanctions are imposed on the complainant, this will regularly constitute a decision within the meaning of Art. 39(1) DA.[773] Under German law, administrative acts (§ 35 VwVfG) are likely to be the primary subject of such actions.[774]

The option granted in Art. 39(2) DA to have the matter resolved by an impartial body is intended to give the Member States the opportunity to set up independent bodies in order to relieve the courts of having to deal with countless actions for failure to act.[775] Legal recourse must also be available against decisions by the impartial bodies, so that the procedure before them is to be seen as a kind of preliminary procedure.[776] In the absence of more detailed provisions on the time limit within which an appeal for failure to act must be lodged or from which it can be lodged, the Member States are free to make their own regulations in this regard within the limits of Art. 47 CFR.[777] The courts of the Member State of the competent authority are responsible for the appeal, Art. 39(3) DA.

d) Sanctions, Art. 40 DA

Art. 40(1)(1) DA provides that the Member States shall lay down rules on penalties applicable to infringements of the provisions of the Data Act and shall take all measures necessary to ensure that they are implemented; the penalties provided for must be effective, proportionate and dissuasive (Art. 40(1) DA). The provisions and measures must be notified to the Commission by **12 September 2025**, which will keep a public and easily accessible register that is updated on an ongoing basis (Art. 40(2) DA).

With regard to the prescribed **triad of effective, proportionate and dissuasive**, it will be possible to fall back on the principles developed for Art. 84 GDPR.[778] According to these principles, sanctions in

772 Roth-Isigkeit, D., 'DA Art. 39', in: BeckOK Datenschutzrecht, para. 3; Remke, C., *MMR* 2024, 117 (120).
773 Roth-Isigkeit, D., 'DA Art. 39', in: BeckOK Datenschutzrecht, para. 3; Remke, C., *MMR* 2024, 117 (120).
774 Remke, C., *MMR* 2024, 117 (120).
775 Roth-Isigkeit, D., 'DA Art. 39', in: BeckOK Datenschutzrecht, para. 11.
776 Roth-Isigkeit, D., 'DA Art. 39', in: BeckOK Datenschutzrecht, para. 11.
777 Roth-Isigkeit, D., 'DA Art. 39', in: BeckOK Datenschutzrecht, para. 8 is based on § 75 VwGO in German law.
778 Roth-Isigkeit, D., 'DA Art. 40', in: BeckOK Datenschutzrecht, para. 2.

the form of fines are particularly **dissuasive** if they exceed the economic advantage gained from the infringement.[779] In contrast, the **effectiveness of** the sanctions must comply with the general principle of effectiveness under EU law (Art. 4(3) TEU).[780] The proportionality of the sanctions is ensured by complying with the prohibition of excessive and insufficient measures.[781]

Art. 40(3) DA contains a non-exhaustive catalogue of various criteria that the authorities[782] must take into account when imposing sanctions; the catalogue of criteria can therefore be understood as a discretionary directive[783]. The catalogue of criteria stipulates that not only the infringement itself, but also the individual circumstances of the party concerned must be taken into account, such as the annual turnover (f) and previous infringements by the party (c). In addition, the recommendations of the EDIB must be taken into account.[784]

For violations of the provisions of Chapters II, III, IV and V DA, data protection supervisory authorities can impose fines within their area of responsibility in accordance with the provisions of Art. 83(5) GDPR, i.e. up to €20 million or 4% of annual worldwide turnover, whichever is higher, which corresponds to the sanction practice of the GDPR (Art. 40(4) DA).

Similarly, Art. 40(5) GDPR authorises the European Data Innovation Board (EDIB) to impose fines within its area of responsibility, although these are limited to EUR 50,000 per infringement and a total of EUR 500,000 in accordance with Art. 66 GDPR.

e) Model contract clauses and standard contract clauses, Art. 41 DA

Furthermore, the Commission will draw up and recommend non-binding model contract clauses for contracts within the scope of the Data Act, Art. 41 DA, by 12 September 2025.[785] These clauses are intended to support SMEs in particular and provide them with practical guidance to facilitate the conclusion of contracts.[786] The focus here is on two objectives in particular: firstly, model contract clauses for data access and use, and secondly, standard contract clauses for cloud computing contracts, both of which are non-binding.[787] The standard contractual clauses should correspond to the FRAND conditions, Art. 41 DA. With Art. 41 DA, the Commission is pursuing an approach similar to the GDPR, where the use of certain standard contractual clauses in practice in the area of international data transfer has been well received.[788]

779 Roth-Isigkeit, D., 'DA Art. 40', in: BeckOK Datenschutzrecht, para. 3.
780 Roth-Isigkeit, D., 'DA Art. 40', in: BeckOK Datenschutzrecht, para. 3.
781 Roth-Isigkeit, D., 'DA Art. 40', in: BeckOK Datenschutzrecht, para. 3.
782 Although Art. 40(3) DA places an obligation on the Member States, this is an editorial error, Roth-Isigkeit, D., 'DA Art. 40', in: BeckOK Datenschutzrecht, para. 4.
783 Roth-Isigkeit, D., 'DA Art. 40', in: BeckOK Datenschutzrecht, para. 6.
784 Rec. 109 Regulation (EU) 2023/2854.
785 European Commission, FAQ DA, p. 26.
786 Rec. 111 Regulation (EU) 2023/2854.
787 v. Roenne, H., 'DA Art. 41', in: BeckOK Datenschutzrecht, para. 4 et seq.
788 v. Roenne, H., 'DA Art. 41', in: BeckOK Datenschutzrecht, para. 2.

An expert group consisting of 17 members has already been set up by the Commission to work on this.[789] Some have criticised the fact that almost all of them have a legal background and therefore, due to a lack of experts in the group from other fields, such as technology or certain industries, the most suitable and technical solution could not be found in practice.[790] With regard to the scope of the mandate to develop model contract clauses, different views are held, particularly on the question of whether the expert group should draft entire contracts or merely submit individual clause proposals.[791] In the opinion of the group of experts, the formulation of entire contract proposals makes sense in order to better protect SMEs.[792]

f) Role of the European Data Innovation Board (EDIB) Art. 42 DA

In addition to this task, the EDIB also fulfils the tasks of Art. 42 DA. It therefore plays a key role in ensuring the standardised application of the Data Act.[793] The EDIB was introduced by Art. 29 DGA, meaning that Art. 42 DA supplements the catalogue of tasks listed in Art. 30 DGA.[794] Within the framework of the Data Act, the EDIB fulfils an advisory and supporting function for the Commission, Art. 42 (a) and (c) DA, and is also intended to support cooperation between different authorities and thus strengthen the uniformity and efficiency of this cooperation, Art. 42(b) DA.

10. Databases containing certain data, Art. 43 DA

The purpose of Art. 43 DA is to protect the effective exercise of the right of users to access and use data and the right to transfer data to third parties by means of the Data Act.[795] Data holders who obtain data through physical components such as sensors of a connected product or a related service should therefore not be able to invoke the sui generis right of a database producer under Art. 7 of Directive 96/9/EC (Database Directive), Art. 43 DA, and thus not be able to restrict the rights to data use and disclosure provided for in the Data Act.[796]

Initial uncertainties exist as to whether Art. 43 DA should be a clarification or a legal amendment to the Database Directive.[797] In particular, difficulties arise from the fact that Art. 7(1) of Directive 96/9/EC places the "procurement" of data under protection and the ECJ has concluded from this that the generation of data does not fall under this protection.[798] With regard to machine-generated data, as well as data

789 https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3840.
790 v. Roenne, H., 'DA Art. 41', in: BeckOK Datenschutzrecht, para. 41.
791 v. Roenne, H., 'DA Art. 41', in: BeckOK Datenschutzrecht, para. 11 et seq.
792 https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/95647/download; v. Roenne, H., 'DA Art. 41', in: BeckOK Datenschutzrecht, para. 12.
793 Rec. 110 Regulation (EU) 2023/2854.
794 v. Roenne, H., 'DA Art. 41', in: BeckOK Datenschutzrecht, para. 11 et seq.
795 Rec. 112 Regulation (EU) 2023/2854.
796 Rec. 112 Regulation (EU) 2023/2854.
797 Kim, D., *MMR* 2024, 87 (88).
798 CJEU, 9 November 2004, C-203/02, The British Horseracing Board Ltd & Ots v. William Hill Organization Ltd = CJEU *MMR* 2005, 29; Kim, D., *MMR* 2024, 87 (88).

obtained or generated by connected products and related services, this raises the question of whether the reading of data is considered to be the generation of new data and therefore Art. 43 DA only clarifies that this data does not fall under Art. 7 of Directive 96/9/EC, or whether it is considered to be the acquisition of existing data within the meaning of Art. 7(1) of Directive 96/9/EC, so that Art. 43 DA constitutes a special regime for data obtained or generated by connected products or related services.[799]

In practice, it could also be difficult to apply the standard in the context of "mixed" databases, whose data fall within the scope of the Data Act on the one hand, but also contain data that are accessible to a property right under Art. 7 of Directive 96/9/EC on the other.[800] In addition, it could be further problematic whether only the data exempt from Art. 43 DA itself or also data generated on its basis are not subject to the protection of Art. 7 Directive 96/9/EC.[801] Art. 43 DA is not applicable in the B2G relationship.[802]

11. Final provisions, Art. 44–50 DA

Obligations to provide data on the basis of Union legislation that entered into force by 11 January 2024 and delegated or implementing acts based thereon remain unaffected by the scope of the Data Act, Art. 44(1) DA. Special data law takes precedence, Art. 44(2) DA.[803] With the exception of Chapter V DA, this applies in particular to data law relating to scientific research, Art. 44(3) DA.

The powers necessary for the adoption of delegated acts are conferred on the Commission for an indefinite period, Art. 45(1), (2) DA. However, this delegation is revocable, Art. 45(3) DA. Further procedural provisions apply, Art. 45(4)–(6) DA.

Furthermore, certain legal acts will be amended to the extent that the Data Act is now also covered, Art. 47, 48 DA. The Commission will evaluate the Data Act by 12 September 2028, Art. 49 DA. Based on this evaluation, it may submit a legislative proposal to amend the Data Act. Art. 49(4) DA. The Data Act entered into force on 11 January 2024 in accordance with Art. 50 DA and applies from 12 September 2025 with a few exceptions.

12. Summary and implications for practice

The Data Act aims to create a single market for data through a differentiated set of rights and obligations for the players in the IoT data cycle. The European Commission has made ambitious forecasts: For example, more efficient data access in the B2B sector is expected to generate added value of 185 billion euros between 2021 and 2030.[804] In the best-case scenario, the EU-wide gross domestic product could

799 Kim, D., *MMR* 2024, 87 (88) et seqq; Richter, H., 'DA Art. 43', in: BeckOK Datenschutzrecht, para. 13.
800 For details see: Richter, H., 'DA Art. 43', in: BeckOK Datenschutzrecht, para. 26 et seq.; Wiebe, A., *GRUR* 2023, 227 (230).
801 Richter, H., 'DA Art. 43', in: BeckOK Datenschutzrecht, para. 30.
802 Richter, H., 'DA Art. 43', in: BeckOK Datenschutzrecht, para. 1, 31.
803 Rec. 115 of Regulation (EU) 2023/2854.
804 European Commission, Impact Assessment Report Data Act, p. 12.

increase by up to 273.1 billion euros.[805] However, it is not yet possible to conclusively assess whether these targets will actually be achieved. Academics and practitioners are divided in their assessment of the Data Act, with criticism prevailing. Some experts criticise the lack of ambition of the act, as data holders and manufacturers can continue to dictate the terms of contracts.[806] Others see the Data Act as consolidating existing power structures[807] or even endorsing them[808]. There are also fears that trade secrets could be jeopardised.[809]

Nevertheless, the Data Act is seen by some scientists as a "step in the right direction"[810] and is viewed positively as an "innovative and courageous legal instrument"[811]. However, the economic cost of implementation is considered to be considerable and, as expected, has been criticised by practitioners.[812] With regard to practical implementation, parallels are already being drawn with the implementation of the requirements of the GDPR from 2017.[813]

Despite the possible simplifications through future model contract clauses from the Commission, key legal issues remain unresolved, leading to considerable legal uncertainty. One of the key questions is how the courts will deal with so-called **buy-out contracts**.[814] These are agreements in which data holders make access to data dependent on the user's comprehensive assignment of rights to the data. It is currently not possible to conclusively assess whether such clauses are in conflict with the overarching objective of the Data Act to ensure fair access to data and should therefore be considered legally inadmissible, in particular in light of Art. 7(2) DA.

A further problem arises with regard to the obligation to technically implement **direct data access** in accordance with Art. 3(1) DA.[815] It is unclear under what conditions manufacturers are obliged to set up technical interfaces for direct access to data and what consequences breaches of this obligation could have.[816]

In addition, the situation in which the data holder and manufacturer are not the same person raises legal questions.[817] In practice, this could lead to conflicts if the manufacturer is not prepared to grant the data holder the necessary access to the data generated by the product. This also concerns the tension between the rights of the user and the rights of the manufacturer.

---

805 European Commission, Impact Assessment Report Data Act, p. 40.
806 Kerber, W., *JoAE* 2024, 1 (6) et seq.
807 Müller, J., *RDi* 2024, 297 (304).
808 Kerber, W., *GRUR Int.* 2023, 120 (128); Specht-Riemenschneider, L., *MMR* 2022, 809 (818).
809 Pauly, D.A./Wichert, F./Baumann, J., *MMR* 2024, 211 (216).
810 Translated from Hennemann, M. et al, Data Act, p. 15.
811 Antoine, L., *CR* 2024, 1 (8).
812 Weinhold, R./Schröder, C. *ZD* 2024, 306 (311).
813 DIHK, Statement on the Data Act-E, p. 2.
814 See 4 b) aa).
815 See 4 c) aa) (1).
816 See 4 c).aa) (2).
817 See 4 c) bb) (3).

The **prohibition of misuse** under Art. 4(10) DA poses a further challenge.[818] The scope of this prohibition and the question of when data access or use constitutes misuse still needs to be clarified by case law. It is particularly unclear to what extent companies can attempt to control access to data through contractual arrangements without fulfilling the requirements of the misuse offence.

Furthermore, the concretisation of the **FRAND standard** (Art. 8(1) DA), which is intended to ensure fair, reasonable and non-discriminatory access to data, is unclear.[819] It remains unclear how this standard is applied in practice and which criteria are used to decide whether access to data must be granted under these conditions.

Finally, the question arises as to whether the data holder's right to consideration under Art. 9(1) DA can be circumvented if the user requests data in accordance with Art. 4(1) DA and passes it on to a third party.[820] In practice, this could result in the data holder not receiving adequate consideration for their data, which could lead to considerable economic disadvantages.

The rules on switching between data processing services will have a significant impact on practice and make an important contribution to the emerging data economy law. It is imperative that companies already begin to adapt their services to align with the impending regulations that are scheduled to come into effect on 12 September 2025. This applies in particular to the change and drafting of contractual clauses within the meaning of Art. 25 DGA.[821] In practice, checklists or catalogues of requirements can be used here.[822] Technical adjustments and the consideration of exceptions under Art. 31 DA are also important.[823] In addition, companies should keep a constant eye on the central database created by the Commission for harmonised standards and common specifications, as this will be constantly updated.[824]

The standard contractual clauses to be drawn up by the Commission in accordance with Art. 41 DA are also eagerly awaited; initial consultations on this are already taking place.[825] The clauses are intended to eliminate uncertainties in the application of Art. 13 DA and reduce transaction costs for data holders and users. Until then, it is recommended to use soft law instruments such as the ALI-ELI Principles or UNCITRAL rules. For the information obligations arising from Chapter VI, the use of an information creation and management system is recommended.[826] For the information and provision obligations, providers could make this information available in a customer area on the website – after the customer

818 See 4 c) cc).
819 See 4 d) bb) (1) (a).
820 See 4 d) cc).
821 Piltz, C./Zwerschke, J., *CR* 2024, 153 (156) et seq.
822 Piltz, C./Zwerschke, J., *CR* 2024, 153 (155) et seq.
823 Heinzke, P., *BB* 2024, 1291 (1296).
824 European Commission, FAQ DA, p. 32.
825 https://digital-strategy.ec.europa.eu/en/events/series-webinars-data-act-contracts.
826 Piltz, C./Zwerschke, J., *CR* 2024, 153 (157).

has registered – and obtain confirmation that they have taken note of the information via a pop-up window or a checkbox.[827]

[827] Schmidt-Wudy, F., 'DA Art. 26', in: BeckOK Datenschutzrecht, para. 12.1.

II. The Relationship of the Data Act to the General Data Protection Regulation and Trade Secrets Protection Law

Bibliography

Andjic, M., "Geheimnisschutz Ade? – Auswirkungen der Datenzugangsansprüche nach dem Data Act auf den Schutz von Geschäftsgeheimnissen," *ZdiW* 2024, 68; Antoine, L.,"Datenzugang im Spannungsfeld zwischen DS-GVO, Geschäftsgeheimnisschutz und Datenbankherstellerrecht – Achillesferse des Data Act in der Praxis?" *CR* 2024, 73; Antoine, L., "Datenzugangsrechte im finalen Data Act – Fortschritt, Rückschritt, neue Fragen? – Schlüssel zur Förderung datengetriebener Geschäftsmodelle?" *CR* 2024, 1; Assion, S., & Willecke, L., "Der EU Data Act – Die neuen Regelungen zu vernetzten Produkten und Diensten," *MMR* 2023, 805; Bomhard, D., "Der Anwendungsbereich des Data Act," *MMR* 2024, 71; Borges, G., & Keil, U. (eds.), Rechtshandbuch Big Data – Grundlagen, Rechtsfragen, Vertragspraxis, 1st ed., Nomos 2023; Ehmann, E., & Selmayr, M. (eds.), Datenschutz-Grundverordnung, 3rd ed., C.H. Beck 2024; European Commission, Study on the legal protection of trade secrets in the context of the data economy – final report, 2022, accessible at: https://op.europa.eu/en/publication-detail/-/publication/c0335fd8-33db-11ed-8b77-01aa75ed71a1/language-en; Franzen, M., Gallner, I., & Oetker, H. (eds.), Kommentar zum europäischen Arbeitsrecht, 5th ed., C.H. Beck 2024; Götz, M., "Data Act-Entwurf und Ansprüche auf den Zugang zu Fahrzeugdaten – Im Spannungsverhältnis von Automobilhersteller, Fahrzeugflottenbetreiber und Fahrzeugführer unter besonderer Berücksichtigung der Vorgaben der DS-GVO," *RAW* 2023, 98; Götz, M., & Blöink, S., "Datenvertrag: Lösungsansatz für das Spannungsfeld zwischen Data Act und DS-GVO – Bewältigung datenschutzrechtlicher Herausforderungen bei Datenzugangsansprüchen," *MMR* 2024, 451; Grapentin, S., "Datenzugangsansprüche und Geschäftsgeheimnisse der Hersteller im Lichte des Data Act," *RDi* 2023, 173; Grützmacher, M., "Datenzugang und Geschäftsgeheimnisschutz," *CR* 2024, 281; Hartl, K., & Jetzen, F., "Der Data Act, Datenzugangsrechte und Art. 6 DS-GVO," *ZdiW* 2023, 65; Herrmann, P., & Schlingloff, J. (eds.), Münchener Kommentar zum Lauterkeitsrecht, Band 1, 3rd ed., C.H. Beck 2020; Hennemann, M., & Steinrötter, B., "Der Data Act – Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen," *NJW* 2024, 1; Hoeren, T., & Muenker, R. (eds.), Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), 1st ed., De Gruyter 2021; Hoeren, T., Sieber, U., & Holznagel, B. (eds.), Handbuch Multimedia-Recht, 61st ed., C.H. Beck 2024; Koós, A., "Die europäische Geschäftsgeheimnis-Richtlinie – ein gelungener Wurf? – Schutz von Know-how und Geschäftsinformationen – Änderungen im deutschen Wettbewerbsrecht," *MMR* 2016, 224; Krause, T., & Maasjeost, H., "Vereinbarkeit von Data Act und DS-GVO," *ZD-Aktuell* 2024, 01494; Köhler, H., Bornkamm, J., & Feddersen, C. (eds.), Gesetz gegen den unlauteren Wettbewerb, 14th ed., Band 13a, C.H. Beck 2024; Kühling, J., & Buchner, B. (eds.), DS-GVO, BDSG – Kommentar, 4th ed., C.H. Beck 2024; Leistner, M., & Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors – Study requested by the JURI committee, 2022, accessible at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf; Metzger, A., & Schweitzer, H., "Shaping Markets: A Critical Evaluation of the Draft Data Act," *ZEuP* 2023, 42; Pauly, D., Wichert, F., & Baumann, J., "Schutz von Geschäftsgeheimnissen nach dem Data Act," *MMR* 2024, 211; Sattler, A., "Notwendige Synchronisierung von Data Act und DS-GVO – Auf die Einwilligung kommt es an," *CR* 2024, 383; Schemmel, F., "Data Act und DS-GVO: Ziemlich beste Feinde?" *CB* 2024, 301; Specht-Riemenschneider, L., "Der Entwurf des Data Act – Eine Analyse der vorgesehenen Datenzugangsansprüche im Verhältnis B2B, B2C und B2G," *MMR* 2022, 809; Specht-Riemenschneider, L., "Datennutz und Datenschutz: zum Verhältnis zwischen Datenwirtschaftsrecht und DS-GVO," *ZEuP* 2023, 638; Steinrötter, B., "Verhältnis von Data Act und DS-

GVO," *GRUR* 2023, 216; Taeger, J., & Gabel, D. (eds.), DS-GVO, BDSG, TTDSG – Kommentar, 4th ed., R&W Verlag 2022; Tinnefeld, C., & Vogel, A., "Auswirkungen des Datenschutzrechtes auf Datennutzungs- und Datenzugangsrechte nach dem Data Act," *ZdiW* 2024, 61; Wiebe, A., "Der Data Act – Innovation oder Illusion?" *GRUR* 2023, 1569; Wiedermann, N., Conrad, T., & Salemi, S., "Bereitstellung von Daten nach dem Data Act – offene Fragen und verbleibende Probleme," *K&R* (2024), 157; Wolff, H. A., Brink, S., & v. Ungern-Sternberg, A. (eds.), Beck'scher Online-Kommentar Datenschutzrecht, 49th ed., Status: 1 August 2024, C.H. Beck.

1. Introduction

Art. 1(5) DA stipulates that the provisions of the Data Act apply without prejudice to Union law and national law on the protection of personal data, privacy, confidentiality of communications and the integrity of terminal equipment used for personal data.[828] In other words, the provisions of the GDPR and the ePrivacy Directive in particular must also be applied without restriction within the framework of the Data Act. As the provisions of the Data Act pursuant to Art. 1(2) DA apply to both personal and non-personal product and related service data, the scope of the GDPR is also regularly opened in the case of personal data. A processing basis within the meaning of Art. 6 GDPR is therefore always required for the transfer of IoT data with a personal reference on the basis of the Data Act. At the same time, the comprehensive approach of the Data Act reveals a tension with the data protection processing principles of Art. 5 et seq. GDPR.[829] The Data Act (supposedly) resolves this tension through overriding the provision of Art. 1(5) DA, according to which the provisions of the GDPR should take precedence in the event of an objection.

There is also potential for conflict in the relationship between the data access regulations of the Data Act and the regulations on the protection of trade secrets, which have their legal basis in the European Union in the Directive on the Protection of Trade Secrets (hereinafter: Trade Secrets Directive). The Trade Secrets Directive, which was implemented in Germany with the Trade Secrets Protection Act (GeschGehG), is, in particular, an expression of the entrepreneurial freedom guaranteed in Article 16 of the Constitutional Law (Grundgesetz).[830] A conflict between the two regulatory regimes regularly arises when the data to be made available on the basis of the Data Act affects the data holder's business secrets. Despite considerable criticism during the legislative process, the EU legislator decided – unlike with the Open Data Directive, for example, and despite corresponding proposals – against creating a fundamental exception to the scope of the DA for trade secrets.[831] Instead, the DA now provides a system of individual regulations and selective exceptions regarding individual access rights, for example in Art. 4(6–8) DA

828 See also Rectical 7 Regulation (EU) 2023/2854.
829 Bomhard, D., *MMR* 2024, 71, (72); Götz, M./Blöink, S., *MMR* 2024, 451 (452); Wiebe, A., *GRUR* 2023, 1569 (1573).
830 Rec. 1, 2, 34 Directive (EU) 2016/943; Hoeren, T./Münker, R./Hoeren, T., GeschGehG, 1st ed. 2021, Section 1 para. 2, 5.
831 Pauly, D./Wichert, F./Baumann, J., *MMR* 2024, 211.

or Art. 5(9–11) DA. Consequently, data that is the subject of the access claims regulated in the DA can also be trade secrets within the meaning of the Trade Secrets Directive and limit the data access.

Data protection law in the form of the GDPR and the regulations on the protection of trade secrets therefore act to a certain extent as a limiting provision in relation to the data access regulations of Art. 4 et seq. DA. Compliance with data protection regulations is of particular importance for companies, as liability on the basis of the GDPR can also be considered in view of the "principle of non-affection" standardised in Art. 1(5) DA.[832] In contrast, the provisions on the handling of trade secrets are relevant for companies because, under certain circumstances, they can thwart the data access claims regulated in the Data Act (Art. 4(7) DA). Against this background, a differentiated assessment of the relationship between both provisions and the Data Act is required.

2. Data Act and GDPR

a) Conflict between Data Act and GDPR for mixed data sets

A central problem is the competing regulation in Art. 1(5) DA, which on one hand emphasises that the Data Act applies "without prejudice" to data protection law, but at the same time establishes a priority regulation in favour of the GDPR in recital 7. This precedence always applies when personal data is affected, which in practice leads to considerable demarcation problems. This is particularly relevant for so-called **mixed data sets**, which contain both personal and non-personal data and therefore affect the scope of both legal acts.[833] In practice, mixed data sets can occur in various contexts: One example of this is the usage data of connected vehicles, where data such as location history, driving behaviour and speed are recorded. The combination of technical data with location information often makes it possible to draw conclusions about the owner or driver.[834] Taking into account the prevailing opinion in case law[835] and literature on the relative personal reference,[836] in this context the question arises whether the assessment of the personal reference of data depends on the perspective of the data owner or the perspective of the data user.[837]

Another example concerns virtual assistants that collect voice and interaction data from the user in order to provide specific services. Such data may contain information about the user's interactions with other connected devices and may also allow to draw conclusions about the user's identity, making it partially personalised.

---

832 On the Commission's draft Specht-Riemenschneider, L., *ZEuP* 2023, 636 (663).
833 Rec. 34 Regulation (EU) 2023/2854.
834 Schild, H., 'GDPR Art. 4', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 21; Götz, M., *RAW* 2023, 98 (102).
835 See most recently CJEU, 9 Nov. 2023, case - C-319/22, para. 49.
836 For the current state of opinion, see Gola, P./Heckmann, D./Gola, P., DS-GVO, 3rd. ed. 2022, Art. 4 para. 20 et seq.
837 Assion, S./Willecke, L., *MMR* 2023, 805 (810).

b) Conflict of laws, Art. 1(5) DA

The relationship between the DGA and the GDPR is primarily determined by Art. 1(5) DGA. Accordingly, the DGA initially applies irrespective of the GDPR and the ePrivacy Directive; however, in the event of a conflict between the two regulations, the GDPR takes precedence in accordance with Art. 1(5) DGA.[838] However, a contradiction within the meaning of Art. 1(5) DA – based on the case law of the ECJ on competition law – can only be assumed if a coexistence of the regulations (so-called **collision case**) is not possible under any circumstances.[839] Both provisions must be virtually incompatible with each other and it must not be possible to reconcile them using appropriate formulae.[840] With regard to the relationship between the user's right to data access under Art. 4 GDPR and the right to data portability (Art. 20 GDPR) and the right to erasure under Art. 17 GDPR, the legislator clarifies that the former is to be understood as a supplement to the rights of data subjects under data protection law.[841] The extent to which the provisions of the Data Act can be considered compatible with the principles of data minimisation (Art. 5(1)(b) GDPR), the principle of purpose limitation (Art. 5(1)(c) GDPR) and the principle of storage limitation (Art. 5(1)(e) GDPR) remains unclear.[842] For the principle of data minimisation, the legislator unhelpfully references technical and organisational measures that the persons involved in the processing should take in the recitals.[843] In all other cases, each case of conflict requires a case-by-case assessment.[844]

Inversely, there is also the possibility that the Data Act or the DGA may set stricter requirements for the processing of personal data compared to the GDPR, as long as the requirements are in addition to those of the GDPR and are not intended to replace them.[845] In this respect, the provisions of the Data Act and the DGA can also fill in opening clauses of the GDPR or be taken into account in the interpretation of undefined legal terms and in the context of balancing decisions of the GDPR.[846]

c) Personal roles

The central actors of the Data Act differ from those of the GDPR; in some cases, there may also be overlaps. While the GDPR regulates the relationship between controllers (under data protection law) and data subjects, the access rights in Art. 4 DA and Art. 5 DA standardise the relationship between the user, data controller and, where applicable, third parties.

838 Sattler, A., *CR* 2024, 383 (384).
839 CJEU, 13 Sep. 2018, case - C-54/17 and C-55/17, para. 60; Specht-Riemenschneider, L., *ZEuP* 2023, 643.
840 CJEU, 13 Sep. 2018, case - C-54/17 and C-55/17, para. 60.
841 Rec. 35, 39 Regulation (EU) 2023/2854.
842 Götz, M./Blöink, S., *MMR* 2024, 451 (452); Sattler, A., *CR* 2024, 383 (390).
843 Rec. 8 Regulation (EU) 2023/2854.
844 Schemmel, F., *CB* 2024, 301 (302).
845 Specht-Riemenschneider, L., *ZEuP* 2023, 638 (643).
846 Specht-Riemenschneider, L., *ZEuP* 2023, 638 (643).

aa) Key players of the GDPR

According to the legal definition in Art. 4 No. 7 GDPR**, a controller** is any natural or legal person, public sector body, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data [...]. The essential characteristic of a controller is therefore its power to decide on the purposes and (at least in the sense of a selection decision)[847] on the means of processing.[848] The controller of a data processing operation is subject in particular to the obligations standardised in Art. 26, 28 et seq. GDPR standardised obligations of the GDPR.[849]

The **data subject**, on the other hand, is the person whose personal data is affected by the processing in accordance with Art. 4 No. 1 GDPR.

bb) Key players in the DA

The DA also independently defines the key players that it authorises and obligates.

According to Art. 2 No. 13 DA, a **data holder** is "a natural or legal person that has the right or obligation [...] to use and make available data [...] which it has retrieved or generated during the provision of a related service".

According to Art. 2 No. 12 DA, **a user** is a "natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services."

In addition, the DA defines the term **data recipient** in Art. 2 No. 14 DA as a person to whom data is made available by the data holder for commercial, business, craft or professional purposes without being a user.

Overlaps arise with the term "data subject". Here, the legislator has expressly referred to the definition in Art. 4 No. 1 GDPR in Art. 2 No. 11 DGA.

cc) Tension between the personal roles

The distinction between personal and non-personal data also has an impact on the structure of persons in the Data Act, as the controller within the meaning of Art. 4 No. 7 GDPR will often also be the data holder within the meaning of Art. 2 No. 13 DGA.[850] The user (Art. 2 No. 12 DA) can also be the same person as the data subject within the meaning of the GDPR, but often will not be.[851] Joint controllership

847 Kühling, J./Buchner, B./Hartung, J., DS-GVO, 4th ed. 2024, Art. 26 para. 13.
848 Hoeren, T./Sieber, U./Holznagel, B./Helfrich, M., Handbuch Multimedia-Recht, 62nd ed. 2024, 16.1 para. 36.
849 Hoeren, T./Sieber, U./Holznagel, B./Helfrich, M., Handbuch Multimedia-Recht, 62nd ed. 2024, 16.1 para. 36.
850 Steinrötter, B., *GRUR* 2023, 216 (219).
851 Sattler, A., *CR* 2024, 383 (390); Tinnefeld, C./Vogel, A., *ZdiW* 2024, 61 (63).

within the meaning of Art. 26 GDPR can even be considered in cases where the user is not also the data subject, but still has access to the data generated by the product.[852]

There is an area of tension between the GDPR and the DGA, particularly where users and data subjects are not the same person.[853] For example, a third party wishing to use personal data in accordance with the objectives of the GDPR will usually not contact all data subjects themselves for economic reasons alone, but will instead assert its right of access and use against professional users, such as providers of IoT leasing or rental services, whose data records contain a large amount of personal data.[854]

d) Access claims under Art. 4, 5 DA

According to Art. 4(12) DA and Art. 5(7) DA, the data holder's obligation to provide data only exists insofar as there is a valid legal basis for the processing under Art. 6 GDPR or Art. 9 GDPR. This provision reflects the underlying system of data protection law of a prohibition with reservation of authorisation. Art. 1(5) DA clarifies that the provisions of the DA do not constitute an independent authorisation for the processing of personal data and cannot justify unlimited storage.[855]

Consequently, the lawfulness of the use, provision and disclosure of personal data requires the existence of an authorisation pursuant to Art. 6 or 9 GDPR.[856]

For the user in practice, selecting the right authorisation from the possible circumstances of Art. 6(1) GDPR is likely to prove to be a balancing act.[857]

aa) Consent, Art. 6(1)(a) GDPR

Relevant, but not unproblematic, in this context is the authorisation criterion of consent pursuant to Art. 6(1)(a) GDPR. Accordingly, the processing of personal data is lawful if the data subject has given their consent to the processing for one or more specific purposes. Art. 6(1)(a) GDPR not only comes into consideration as an authorisation criterion for the provision and use of personal data within the meaning of the DA,[858] but is preferred according to recital 7. It states: "In these cases, it may be in the interest of the user to enable the fulfilment of the requirements of Article 6 of Regulation (EU) 2016/679."

(1) Voluntariness

The data protection principle of informational self-determination and transparency requires that the consent of data subjects is voluntary. This signifies that the data subject must retain the autonomy to consent

852 Steinrötter, B., *GRUR* 2023, 216 (220).
853 Antoine, L., *CR* 2024, 73 (74); Sattler, A., *CR* 2024, 383 (390); Wiedermann, N./Conrad, T./Salemi, S., *K&R* 2024, 157 (158).
854 Sattler, A., *CR* 2024, 383 (390).
855 Hennemann, M./Steinrötter, B., *NJW* 2024, para. 28; Sattler, A., *CR* 2024, 383 (384).
856 Götz, M./Blöink, S., *MMR* 2024, 451 (454).
857 Schemmel, *CB* 2024, 301 (305).
858 Rec. 34 Regulation (EU) 2023/2854.

to the processing or withhold their consent.[859] The data subject only has such a free choice if they are able to refuse or withdraw their consent without suffering any disadvantages.[860]

Consent is involuntary, for example, in the event of an imbalance between the data subject and the controller or in the event of a breach of the so-called **prohibition of tying** under Art. 7(4) GDPR.[861] Accordingly, when assessing whether consent has been given voluntarily, the most importance must be placed on whether, among other things, the fulfilment of a contract is dependent on consent to the processing of personal data that is not necessary for the fulfilment of the contract. A contract should therefore not be made dependent on consent that is not necessary for the fulfilment of the contract.[862]

However, the scope and extent of Art. 7(4) GDPR are controversial. While some literature comprehends the prohibition of tying as a strict prohibition,[863] the prevailing perspective in the literature is that Art. 7(4) GDPR should not be interpreted as an absolute prohibition, but rather as a requirement to take into account the specific circumstances of the individual case and, in particular, in the case of a link between contract and consent, to pay particular attention to the requirement of voluntariness.[864]

Furthermore, consent must not only be voluntary, but also sufficiently specific and relate to specific processing purposes. This is likely to be particularly problematic in complex processing and access structures.[865]

(2) Practical relevance

In the event that the user is also the data subject, the request for provision in accordance with Art. 4(1) DA and the request for disclosure pursuant to Art. 5(1) DA, as assumed by Federal Data Protection Commissioner *Specht-Riemenschneider*,[866] should be interpreted as being based on the implied consent of the data subject.[867] This is particularly supported by the wording of Art. 4(12), Art. 5(7) DA, according to which the data controller "only" requires a legal basis for the provision or disclosure of personal data if the user and the data subject do not coincide. Conversely, it can be deduced that in instances where the user is also the data subject, a legal basis as defined in recitals 7 and 34 DA remains necessary. This basis can be derived from the concept of implied consent, which is widely acknowledged and accepted in such circumstances.[868]

---

859 Taeger, J./Gabel, D./Arning, M./Rothkegel, T., DS-GVO, 4th ed. 2024, Art. 4 para. 303.
860 Rec. 42 Regulation (EU) 2016/679.
861 Rec. 43 Regulation (EU) 2016/679.
862 Taeger, J./Gabel, D./Arning, M./Rothkegel, T., DS-GVO, 4th ed. 2024, Art. 4 para. 304 et seqq.
863 Taeger, J./Gabel, D./Arning, M./Rothkegel, T., DS-GVO, 4th ed. 2024, Art. 4 para. 307, Art. 7 para. 97 et seq.
864 Sattler, A., *CR* 2024, 383, (391).
865 Antoine, L., *CR* 2024, 73 (74).
866 Specht-Riemenschneider, L., *MMR* 2022, 809 (810).
867 Schemmel, F., *CB* 2024, (301) 305.
868 Schemmel, F., *CB* 2024, (301) 305.

Since the data holder would have to prove the granting of consent and its existence at the time of making the data available, Art. 6(1)(1)(a) GDPR cannot be considered an unrestricted basis for authorisation for practical reasons.[869]

In the event that the user and data subject are not one and the same entity, consent, which is required to be both voluntary and informed, in addition to being capable of being revoked at any time, as outlined in Art. 7 of the GDPR, does not provide a legally secure and practical basis for authorisation.[870]

bb) Fulfilment of a contract, Art. 6(1)(b) GDPR

According to Art. 6(1)(b) GDPR, the processing of personal data is also lawful if it is necessary for the performance of a contract to which the data subject is party or in order to take steps necessary prior to entering into a contract. The standard therefore seems particularly suitable as a legal basis for the use of data within the meaning of the DA, as Art. 13 DA and Art. 14 DA require a contractual agreement between users and the data controller anyway.[871]

However, the prerequisite is that the data subject must be a party to the contract in relation to the data controller, which only applies to cases in which the data subject is also a user and therefore severely restricts the scope.[872]

In addition, the ECJ ruled that a restrictive interpretation is required with regard to Art. 6(1)(1)(b) GDPR. The standard must be interpreted to the effect that "the processing of personal data can be regarded as necessary for the performance of a contract [...] within the meaning of that provision only if that processing is objectively necessary for the fulfilment of a purpose which is an integral part of the contractual performance intended for those users, so that the main subject matter of the contract could not be fulfilled without that processing."[873] This narrow interpretation of necessity within the meaning of Art. 6(1)(b) GDPR takes into account the ECJ's assessment that consent pursuant to Art. 6(1)(a) GDPR should generally take precedence as a basis for authorisation. Therefore, the possibility of applying Art. 6(1)(b) GDPR as a basis for authorisation within the meaning of Art. 4(12) DA and Art. 5(7) DA is primarily limited to cases of so-called **consent fatigue**.[874] If, for example, regular data processing is required on the basis of a contract, it would be an unreasonable and exhaustive burden to require a declaration of consent for each individual processing operation.[875] Beyond that, Art. 6(1)(b) GDPR is usually not suitable as a legal basis due to the restrictive interpretation of the ECJ.[876]

869 Tinnefeld, C./Vogel, A., *ZdiW* 2024, 61 (66).
870 Schemmel, F., *CB* 2024, (301) 305.
871 The fact that the legislator also sees Art. 6(1)(b) DA as a possible legal basis for uses within the meaning of the DA can be seen from Rec. 34 Regulation (EU) 2023/2854; Sattler, A., *CR* 2024, 383 (387).
872 Schemmel, F., *CB* 2024, (301) 305.
873 CJEU, 4 Jul. 2023, case - C-252/21, *NJW* 2023, p. 2997.
874 Sattler, A., *CR* 2024, 383 (388).
875 Sattler, A., *CR* 2024, 383 (388).
876 Tinnefeld, C./Vogel, A., *ZdiW* 2024, 61 (66).

cc) Fulfilment of a legal obligation, Art. 6(1)(c) GDPR

The legality of Art. 6(1)(c) GDPR, on the other hand, is of comparatively little relevance in the context of the use, provision and disclosure of personal data on the basis of the DA. Although (c) permits processing if it is necessary to fulfil a legal obligation of the controller, the DA itself cannot serve as a legal basis.[877] This follows from the wording of Art. 4(12) DA and Art. 5(7) DA. Accordingly, there must be a legal basis for processing under Art. 6 GDPR in order for personal data to be provided to the user by the data holder.[878] It would be contradictory if the DA itself could be considered a legal obligation within the meaning of Art. 6(1)(c) GDPR. Recital 7 of the GDPR clarifies that this assessment is in line with the EU legislator. According to this, the GDPR expressly "does not constitute a legal basis for the collection or generation of personal data by the data holder." Furthermore, "this Regulation does not create a legal basis for providing access to personal data or for making personal data available to a third party and should not be understood as conferring any new right on the data holder to use personal data generated by the use of a connected product or related service" where "the user is not the data subject".[879]

Since the GDPR does not constitute a legal basis within the meaning of Art. 4(12) DA and Art. 5(7) DA, it also cannot justify a public interest within the meaning of Art. 6(1)(e) and Art. 9(2)(g) GDPR.[880]

dd) Legitimate interest, Art. 6(1)(f) GDPR

For constellations in which the data subject and the user are not identical, only the overriding legitimate interest within the meaning of Art. 6(1)(f) GDPR remains as a de facto right of access.[881]

This authorisation entitles the controller to process personal data if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data. As a catch-all provision, the standard requires a balancing of interests, taking into account the circumstances of the specific individual case.[882] Data processing is lawful if the controller's interest in processing outweighs the data subject's interest in protection.

The Data Act's interest in the extensive and efficient use and transfer of personal data, which the data holder's obligations to provide data pursuant to Art. 4(12) DA and Art. 5(7) DA are based on, can generally be considered a suitable processing interest within the meaning of Art. 6(1)(f) GDPR.[883] Federal Data Protection Commissioner *Specht-Riemenschneider* sees in the standardisation of access, provision and forwarding claims the expression of the legislator that the data processing interest should in principle be "at least of equal importance" to the data subject's interest and that the requirements of Art. 6(1)(f)

877 Sattler, A., *CR* 2024, 383 (385).
878 Sattler, A., *CR* 2024, 383 (385).
879 Rec. 7 Regulation (EU) 2023/2854.
880 Tinnefeld, C./Vogel, A., *ZdiW* 2024, 61 (66); Sattler, A., *CR* 2024, 383 (385).
881 Steinrötter, B., *GRUR* 2023, 216 (226).
882 Ehmann, E./Selmayr, M./Heberlein, J., DS-GVO, 3rd ed. 2024, Art. 6 para. 40.
883 Sattler, A., *CR* 2024, 383 (388).

GDPR will therefore generally be met.[884] However, as with any balancing of interests, a decision must ultimately be made on a case-by-case basis.[885]

Basing the provision of personal data on Art. 6(1)(f) GDPR harbours some risks.

On the one hand, there is currently a lack of reliable and differentiated conditions for application. Despite the fact that the case law of the ECJ made the scope more concrete, meaning hat Art. 6(1)(f) GDPR can only be considered as a basis for processing to the extent that data subjects can reasonably expect the processing,[886] a wide potential scope remains, which complicates the practical application.[887]

On the other hand, the ECJ generally considers a narrow interpretation of Art. 6(1)(f) GDPR to be necessary.[888] If the interest in the processing does not clearly prevail, it is therefore often difficult for the controller to foresee whether the processing is lawful or not in the sense of provision in accordance with Art. 4(12)DA and Art. 5(7)DA. The practical applicability of the authorisation is usually risky, particularly due to the high liability risk that exists in the context of the interface between the DA and the GDPR, as both regulations provide for fines for violations.[889]

ee) Summary

The requirement to provide non-personal data in accordance with Art. 4(1), 5(1) DA, which is subject to a financial penalty, is closely related to the preventive prohibition of processing personal data under the GDPR, which is also subject to a financial penalty.[890] The GDPR restricts the access rights of the Data Act in such a way that "there is currently no apparent legal basis under data protection law that could guarantee the implementation of user requests in accordance with Art. 4(1) DA, Art. 5(1) DA in a legally secure manner."[891] Since the core objective of the Data Act is sharing data and creating a European internal market, the data controller cannot argue a lack of legal basis under the data protection law if it wishes to refuse access, provision and transfer claims under the Data Act.[892] The data controller is therefore forced to seek a legal basis under data protection law in the tense relationship between the GDPR and the Data Act.

If the user and the data subject are the same person, the data access request pursuant to Art. 4(1), Art. 5(1) GDPR also constitutes implied consent pursuant to Art. 6(1)(a) GDPR, Art. 7 GDPR. However, here too, the high requirements that the GDPR places on consent in Art. 6, 7 GDPR and the strict case law can make it difficult to use consent as a reliable legal basis in practice. Due to the narrow scope and its restrictive interpretation by the ECJ, data processing for the fulfilment of a contract pursuant to

884 Specht-Riemenschneider, L., *MMR* 2022, 809 (811); doubting Steinrötter, B., *GRUR* 2023 (223).
885 Schemmel, F., *CB* 2024, 301 (306).
886 CJEU, 4 Jul. 2023, case - C-252/21, *NJW* 2023, p. 2997
887 Sattler, A., *CR* 2024, 383, (388 et seq.).
888 CJEU, 4 Jul. 2023, case - C-252/21, *NJW* 2023, p. 2997; CJEU, 24 Feb. 2022, case - C-175/20, EuZW 2022, p. 527.
889 Tinnefeld, C./Vogel, A., *ZdiW* 2024, 61 (66).
890 Steinrötter, B., *GRUR* 2023, 216 (223).
891 Steinrötter, B., *GRUR* 2023, 216 (223).
892 Schemmel, F., *CB* 2024, 301 (306).

Art. 6(1)(b) GDPR only comes into question in clearly defined cases of regular data processing with no scope for further processing and is therefore of little practical relevance. As the GDPR itself does not constitute a basis for data access within the meaning of the Data Act, the authorisation provisions of Art. 6(1)(c) and (e) GDPR are also of little practical relevance.

The only possible authorisation for constellations in which the user and the data subject are different requires, even if it is assumed that the data processing interest and the data subject's interest are equal, a case-by-case assessment, which will be difficult in practice and characterised by legal uncertainty due to the lack of clearly defined application requirements and the restrictive case law of the ECJ.

e) Special categories of personal data pursuant to Art. 9 GDPR

Art. 9 GDPR standardises the processing of special categories of personal data and, in relation to Art. 6 GDPR, sets stricter conditions for the lawfulness of data processing (Art. 9(2) GDPR). Art. 9 GDPR defines its scope in para. 1, where data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic and biometric data for the purpose of uniquely identifying a natural person and data concerning health or data concerning a natural person's sex life or sexual orientation are listed as particularly sensitive data.

However, the distinction between particularly sensitive personal data and other personal data is made more difficult by the case law of the ECJ.[893] In the judgement on Meta/BKartA, Art. 9 GDPR is already applied if the data set "contains both sensitive and non-sensitive data" and "is collected as a whole without it being possible to separate the data at the time of collection".[894] It is therefore sufficient for an infringement to occur if only "one sensitive personal data item" is present in a larger data set and no exception under Art. 9(2) GDPR applies.[895]

According to the ECJ, data records already contain sensitive data when users visit websites whose operators use cookies, integrated interfaces or similar storage technologies to collect data about the website visit and the information entered by the user on the website, which allows conclusions to be drawn about particularly sensitive data, such as the user's sexual orientation or political opinion.[896] The accuracy of the sensitive information collected through the processing is irrelevant.[897] It is also irrelevant whether the data controller intends to collect sensitive data when collecting the data.[898]

893 Sattler, A., *CR* 2024, 383 (389).
894 CJEU, 4 Jul. 2023, case - C-252/21, para. 89.
895 Wolff, A./Brink, S./v. Ungern-Sternberg, A. /Albers, M. /Veit, R.-D., DS-GVO, 2nd ed. 2022, Art. 9 para. 17a.
896 Sattler, A., *CR* 2024, 383 (390).
897 CJEU, 4 Jul. 2023, case - C-252/21, para. 89.
898 CJEU, 4 Jul. 2023, case - C-252/21, para. 89.

The problem is that the data holder will rarely have any influence on whether a user, who is also the data subject, uses the relevant product or connected service in such a way that sensitive data is (automatically) generated.

Due to the broad interpretation of sensitive personal data, data holders will have to require users to provide explicit consent in relation to sensitive data before they can authorise access to or use of data.[899]

f) Data access rights (Art. 4, 5 GDPR) and data portability (Art. 20 GDPR)

Another problem area concerns the data access rights under Art. 4 and 5 of the Data Act, which go beyond the rights to data portability under Art. 20 GDPR. While GDPR only grants a right to a one-time data transfer, the Data Act provides for the continuous provision of data in real time. This poses considerable challenges for companies, as the technical and legal feasibility of such continuous data provision are often not given. The distinction between the right to data portability under Art. 20 GDPR and the data access and onward transfer rights under Art. 4 and 5 Data Act (DA) is difficult, as both regimes partly concern the same scope. Art. 4 and 5 DA cannot be interpreted as only covering non-personal data, as the broad definition of "data" in Art. 2 No. 1 DA excludes this.[900] Personal data must be made available in a structured, commonly used and machine-readable format in accordance with both Art. 20 GDPR and Art. 4(1) DA, but the Data Act differs in that it allows for continuous and real-time provision of data. While Art. 12(3) GDPR provides a timeframe of up to one month, the Data Act in Art. 4(1) and Art. 5(1) requires continuous and immediate provision, where relevant and technically feasible. The necessary technical infrastructure (e.g. standardised APIs, data formats, etc.) in particular is crucial for the provision of data in practice and will pose challenges for companies. The regulations on interoperability, for example Art. 33 DA, only address this issue to a limited extent.[901]

g) Legal basis for the processing of personal data in the context of data access claims pursuant to Art. 4, 5 DA and B2G data access pursuant to Art. 14 et seq. DA

Another major problem is the lack of a legal basis in the Data Act for the processing of personal data. The Data Act itself does not create an independent legal basis for the processing of personal data, but refers to the GDPR, in particular Art. 6 GDPR. This means that any processing of personal data that takes place under the Data Act requires a separate legal basis under the GDPR. This can lead to considerable practical problems, especially when data is passed on to third parties or public bodies. Art. 4(12) and Art. 5(7) of the Data Act emphasise this necessity. In the case of a data transfer, the consent of the data subject pursuant to Art. 6(1)(a) GDPR remains the most common means, but this is often difficult to implement in practice.

---

899 Sattler, *CR* 2024, 383 (390).
900 Krause, T./Maasjost, H., *ZD-Aktuell* 2024, 01494; but Drexl et al, Position Statement MPI, p. 105 para. 293.
901 Antoine, L., *CR* 2024, 1 (5).

In literature, the suggestion that Art. 4, 5 DA should be qualified as a legal obligation within the meaning of Art. 6(1)(c) GDPR already came up a while ago.[902] However, the lack of mention in the recitals of the DA[903] speaks against this and in the final version of the Data Act this was explicitly clarified in recitals 7, 34.

The consent of the data subject pursuant to Art. 6(1)(a) GDPR appears to be the most practical tool.[904]

According to recital 69, the provisions of the Data Act are the required processing basis for B2G data access pursuant to Art. 6 (1), (3) GDPR. Art. 6(1)(d) GDPR can also be considered as a basis according to isolated opinions in the literature.[905]

h) Risk of fines

The interaction between GDPR and DA harbours a considerable liability risk in practice. Both the GDPR and the DA provide for fines for violations of their provisions under Art. 83 GDPR and Art. 40 DA. If companies make mistakes when classifying data, they are exposed to a **double liability for fines**. If personal data is incorrectly categorised as non-personal data and therefore used for processing without a legal basis under data protection law, there is a risk of fines under the GDPR (Art. 83 GDPR). Conversely, there is a risk of a breach of the Data Act if companies refuse data access or disclosure requests with reference to the lack of a legal basis under data protection law. This 'liability dilemma' requires careful consideration in individual cases in order to avoid violating either of the two regimes.

In order to minimise the risk of liability due to data protection violations within the meaning of the GDPR, it was common practice until the DA came into force to assume that data was personal in cases of uncertainty regarding the classification of data as personal or non-personal.[906]

However, since the DA came into force, this practice is no longer advisable if the personal nature of data is to be held against a data access request under the DA.[907] If non-personal data is incorrectly categorised as personal data and a data access request is rejected for this reason, this does not constitute a breach of the GDPR. However, it does constitue a breach of the DA, which in turn is also subject to a fine.[908]

---

902 Leistner, M./Antoine, L., IPR and the use of open data: Study requested by the JURI committee, PE 732.266, 2022, p. 69.

903 Assion, S./Willecke, L., *MMR* 2023, 805, 810; Hartl, K./Jetzen, F., *ZDiW* 2023, 65 (67); Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (77).

904 Krause, T./Maasjost, H., *ZD-Aktuell* 2024, 01494.

905 Leistner, M./Antoine, L., IPR and the use of open data: Study requested by the JURI committee, PE 732.266, 2022, p. 111.

906 Götz, M./Blöink, S., *MMR* 2024, 451 (452).

907 Götz, M./Blöink, S., *MMR* 2024, 451 (452).

908 Hennemann, M./Steinrötter, B., *NJW* 2024, para. 27; Götz, M./Blöink, S., *MMR* 2024, 451 (452).

Compliance with the Data Act and the GDPR at the same time would make the sometimes difficult determination of the personal reference superfluous. However, the GDPR and the Data Act have different requirements for information obligations and the requirements for effective consent under data protection law are strict, meaning that this "one-size-fits-all" approach is not practicable.

In the area of conflict between the GDPR and the DGA, requirements and prohibitions are close to each other. The only way to avaoid the risk of fines is categorizing data as personal or non-personal. However, this is often complex and hardly foreseeable for data owners or controllers. In addition, the distinction requires further clarification in case law.[909]

Therefore, the liability dilemma and the "fine trap" are probably best avoided by anonymising the data and thus "switching off" the GDPR;[910] this possibility is also explicitly mentioned in recital 7 DA. The Data Act even requires anonymisation of the data in certain cases (Art. 18(4) DA). However, in practice, anonymisation poses considerable technical requirements that are not always easy to implement.

i) Conclusion

The relationship between the Data Act and the GDPR is complex and characterised by numerous unresolved demarcation issues. Despite the precedence clause introduced in favour of the GDPR, many practical and legal uncertainties remain. Companies must ensure compliance with both the requirements of the Data Act and the GDPR, which is often difficult in practice. Anonymisation is an important way of avoiding conflicts, but in many cases it is not easy to implement. Ultimately, the application of both regimes requires a careful case-by-case assessment and a clear legal strategy to minimise the risks of fines and liability.

3. Data Act and trade secret protection law

With the Directive (EU) 2016/943, the European legislator intended to achieve a minimum harmonisation of the protection of trade secrets under civil law in the EU.[911] It is based on the enabling provision of Art. 114 TFEU and came into force on 5 July 2016. This directive had to be implemented in the member states by 9 June 2018.

In terms of primary law, the Directive (EU) 2016/943 is linked to various fundamental rights of the European Charter of Fundamental Rights. Central to this are the protection of personal data (Art. 8 CFR), freedom of expression and information (Art. 11 CFR), freedom to choose an occupation (Art. 15 CFR), freedom to conduct a business (Art. 16 CFR) and the protection of property (Art. 17 CFR).[912] In particular, the substantive areas of protection of Art. 16 CFR and Art. 17 CFR are affected by the Directive (EU) 2016/943, as trade secrets are economic resources whose use is generally the responsibility

909 Bomhard, D., *MMR* 2024, 71, 74; Tinnefeld, C./Vogel, A., *ZdiW* 2024, 61 (64 et seq.).
910 Schemmel, F., *CB* 2024, 301 (303 et seq.).
911 Hoeren, T./Münker, R./Hoeren, T., GeschGehG, 1st ed. 2021, Art. 1 para. 6; Hoeren, T./Sieber, U./Holznagel, B./Drescher, J., Handbuch Multimedia-Recht, 62nd ed. 2024, 7.9 before Art. 1 para. 20.
912 Rec. 34 Directive (EU) 2016/943.

of the companies themselves.[913] In this respect, the Directive (EU) 2016/943 serves to protect companies and their innovation and – as a result – their competitiveness, which should benefit European competition and the internal market.[914]

The Directive (EU) 2016/943 is divided into four chapters with a total of 21 articles. The first chapter (Art. 1–2 Directive (EU) 2016/943) defines the subject matter and scope of the Directive and provides for definitions. The second chapter (Art. 3–5 Directive (EU) 2016/943) lays down rules on the acquisition, use and disclosure of trade secrets and differentiates between lawful and unlawful acquisition. In its third chapter (Art. 6–15 Directive (EU) 2016/943), the Directive (EU) 2016/943 contains provisions on measures, procedures and legal remedies. In three subsections, these are divided into general provisions, provisional and preventive measures and measures based on a decision on the merits. The fourth and final chapter of the Directive provides for sanctions, reporting obligations and final provisions in Articles 16–21 of the Directive (EU) 2016/943. The Directive is preceded by 40 recitals.

In Germany, the Act on the Protection of Trade Secrets (GeschGehG) came into force on 26 April 2019 as a key implementation of the Directive (EU) 2016/943.

a) Directive (EU) 2016/943

aa) Area

Directive (EU) 2016/943 does not expressly provide for a personal scope . However, according to Art. 1(1) Directive (EU) 2016/943, the Directive is intended to lay down rules "for the protection against the unlawful acquisition, use and disclosure of trade secrets". Subjectively affected are therefore, on the one hand, the trade secret holders within the meaning of Art. 2 No. 2 Directive (EU) 2016/943 and, on the other hand, the infringers within the meaning of Art. 2 No. 3 Directive (EU) 2016/943.[915]

The Directive (EU) 2016/943 lays the foundation for the material scope in its Art. 1(1), which "lays down rules on the protection against the unlawful acquisition, use and disclosure of trade secrets." The term "trade secret" is legally defined in Art. 2 No. 1 of the Directive (EU) 2016/943. Accordingly, trade secrets are:

> *" information which meets all of the following requirements:*
>
> *(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
>
> *b) it has commercial value because it is secret;*

913 Köhler, H./Bornkamm, J./Feddersen, J./Alexander, C., UWG, 42nd ed. 2024, GeschGehG before Art. 1 para. 7.
914 Rec. 1-4 Directive (EU) 2016/943.
915 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art. 1 para. 10.

(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret"

The conditions stated in the definition must be met cumulatively.[916]

However, the Directive (EU) 2016/943 does not expressly define the concepts of acquisition, use and disclosure, so that the EU legislator is called upon to interpret and adjudicate on these issues.[917]

The material scope is therefore initially quite broad and requires concretisation by the Member States.[918] Relevant restrictions arise from Art. 1(2) and (3) Directive (EU) 2016/943. Here, the Directive (EU) 2016/943 expressly standardises various rights and provisions that are not to be affected by it.

According to Art. 1(2)(a) Directive (EU) 2016/943, "the exercise of the right to freedom of expression and information [...]" is not supposed to be affected, which corresponds to Art. 11 CFR. In this respect, the standard is to be categorised as a declaratory commitment to Art. 11 CFR, the significance of which in the context of the Directive (EU) 2016/943 is also expressed in Art. 5(a) Directive (EU) 2016/943.[919] The mobility of employees protected in Art. 1(3) Directive (EU) 2016/943 is also particularly relevant. This restriction of the scope of the Directive (EU) 2016/943 is intended to protect employees' freedom to choose an occupation. On the one hand, they should be able to change the company in which they are employed. On the other hand, they should also be able to utilise the skills and experience acquired in the previous company within the scope of their new employment. So-called "lock-in" effects, i.e. employees being restricted in their mobility and thus in their occupational freedom by de facto restrictions, should be avoided.[920]

Despite the rather detailed restrictions on the scope of the Directive (EU) 2016/943, the Member States still have considerable room for manoeuvre with regard to the material scope, as Art. 1(2) and (3) of the Directive (EU) 2016/943 views not clearly defined acts as lawful are or declares them as lawful, just like Art. 3 to 5 of the Directive (EU) 2016/943 do.[921]

bb) Lawful and unlawful use, Art. 3, 4, 5 Directive (EU) 2016/943

Trade secrets are not protected as an absolute right; instead, unfair exploitation and disclosure is prohibited.[922] In contrast to intellectual property rights, the Directive (EU) 2016/943 does not provide for exclusive rights to trade secrets,[923] but rather defines the circumstances under which trade secrets may be

916 Koós, A., *MMR* 2016, 224 (225).
917 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art. 1 para. 13.
918 EuArbRK/Schubert, C., 5th ed. 2024, Directive (EU) 2016/943 Art. 2 para. 3.
919 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art 1 para. 16 et seq.
920 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art. 1 para. 22.
921 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art. 1 para. 15.
922 In this respect, the Trade Secrets Directive corresponds to Art. 39(2) of the TRIPS Agreement (= Agreement on Trade-Related Aspects of Intellectual Property Rights); Koós, A., *MMR* 2016, 224 (225); MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 preliminary remarks para. 4 et seq.
923 Rec. 16 Directive (EU) 2016/943; MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 preliminary remarks para 8.

lawfully (Art. 3 Directive (EU) 2016/943) or unlawfully (Art. 4 Directive (EU) 2016/943) acquired, utilised or disclosed. Art. 5 Directive (EU) 2016/943 also provides for exceptions to Art. 4 Directive (EU) 2016/943. In this respect, Art. 3–5 form the core part of the Directive (EU) 2016/943.

Art. 3(1) Directive (EU) 2016/943 sets out as a positive list (**whitelist**)[924] when the acquisition of a trade secret is lawful without further consideration. Acquisition is broadly understood to mean "any form of obtaining possession"[925] or, in the case of intangible information, knowledge.[926] The legal elements of Art. 3(1) Directive (EU) 2016/943 appear at first glance to be very differentiated, but allow the Member States considerable room for manoeuvre, in particular due to the provision of Art. 3(1)(d) Directive (EU) 2016/943, according to which any other procedure that is compatible with sound business practice under the given circumstances is considered lawful. The list in Art. 3(1) Directive (EU) 2016/943 is, apart from Art. 3(2) Directive (EU) 2016/943, exhaustive.[927] Art. 3(2) Directive (EU) 2016/943 also regulates the lawful disclosure and use of trade secrets in addition to their lawful acquisition and gives the Member States the option of protecting other overriding interests within their sphere of competence.[928]

Art. 4 Directive (EU) 2016/943 provides for a negative list (also known as a **blacklist**)[929] regulations on the unlawful use of trade secrets. Art. 4(1) Directive (EU) 2016/943 is primarily of declaratory significance with regard to the implementation mandate of the member states.[930] Paragraphs 2–5 provide for specific offences. Unlike (4) and (5), (2) and (3) do not provide for a subjective element. The existence of objective characteristics is sufficient.

Art. 5 of the Directive (EU) 2016/943 provides for a total of four grounds for justification, where the acquisition, disclosure and use of a trade secret is exceptionally not unlawful. In this respect, the Directive (EU) 2016/943 offers the possibility of balancing interests on a case-by-case basis.[931]

b) Relationship between the Directive (EU) 2016/943 and the Data Act

The Data Act defines data in its Art. 2 No. 1 DA so broadly that ultimately any data is covered by the DA.[932] This broad material scope results in an interface between the DA and the Directive (EU) 2016/943; individual data can also fall under trade secret protection.[933] Art. 2 No. 18, 19 DA refers to the Directive (EU) 2016/943 for the basis of a standardised understanding of the term.[934] The actual and

924 Franzen, M./Gallner, I./Oetker, H./Schubert, C., EuArbRK, 5th ed. 2024, Directive (EU) 2016/943 Art. 2 para 2.
925 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Directive Art. 3 para 4.
926 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art. 3 para 4.
927 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art. 3 para 5.
928 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art. 3 para 16.
929 Franzen, M./Gallner, I./Oetker, H./Schubert, C., EuArbRK, 5th ed. 2024, Directive (EU) 2016/943 Art. 4 para 2.
930 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art. 4 para 2.
931 MüKoUWG/Namysłowska, M., 3rd ed. 2020, Directive (EU) 2016/94 Art. 5 para 1.
932 Bomhard, D., *MMR* 2024, 71 (72).
933 Wiebe, A., *GRUR* 2023, 1569 (1573).
934 Schild, M., 'DA Art. 2', in: BeckOK Datenschutzrecht (49th ed. 2024) para 99.

economic significance of data that is subject to the Directive (EU) 2016/943 and is exchanged between companies in practice is increasing.[935]

The relationship between the DA and the Directive (EU) 2016/943 is largely determined by Art. 4(6), (7), (8) DA and Art. 5(9), (10), (11), (12) DA and gives the DA's right of access to data priority over trade secret protection.[936]

The fact that the DA does not standardise a general exception to the DA's access rights for trade secrets does justice to the different protection dimensions of DA and trade secret protection. While the DA's access rights assign de facto positions of control over data, trade secret protection concerns the way in which de facto control is protected.[937] The protection dimension of the DA does not necessarily run counter to that of the Directive (EU) 2016/943.

aa) Requirements for the provision of trade secrets, Art. 4 DA

Art. 4(6), (7), (8) DA regulate the requirements for the provision of trade secrets to the user. Accordingly, trade secrets only have to be disclosed if the necessary protective measures have been taken. Compared to Art. 4(3) DA, which was criticised in particular for the fact that it was unclear when a breach had occurred and what consequences it should entail, the final version of the DA represents a clear specification of the requirements.[938] However, Art. 4(6) DA still does not specify the standard of necessity.[939] Art. 4(6) DA provides for contractual agreements as necessary protective measures, in particular the agreement of appropriate technical and organisational measures between the trade secret holder and the user to protect the trade secrets.[940] According to the recitals of the DA, these include model contractual clauses, confidentiality agreements and strict access protocols.[941] Furthermore, codes of conduct can also be considered.[942]

According to Art. 4(6) DA, it is incumbent on the data holder to determine the data protected as a trade secret *ex ante* before a user agreement is concluded on this basis. This obligation results in an imbalance in relation to the user, as the data holder can easily categorise large data sets as trade secrets and restrict access on this basis. It is true that the data holder may not unreasonably impede the exercise of the user's rights pursuant to Art. 4(4) DA. However, it is questionable whether this provision can do justice to the imbalance.[943]

---

935 European Commission, Study on the legal protection of trade secrets in the context of the data economy - final report, 2022, p. 94.
936 Hennemann, M./Steinrötter, B., *NJW* 2024, 1 (6); Wiebe, A., *GRUR* 2023, 1569 (1573).
937 Müller, J., *RDi* 2024, 297 (298 et seq.).
938 Wiedermann, N./Conrad, T./Salemi, S., *K&R* 2024, 157 (162).
939 Doubtful Hennemann, M/ Ebner, G../Karsten, B./Lienemann, G./Wienroeder, M., Data Act, p. 96.
940 Hennemann, M./Steinrötter, B., *NJW* 2024, 1 (6); Andjic, M., *ZdiW* 2024, 68 (71).
941 Rec. 31 Regulation (EU) 2023/2854.
942 Hennemann, M/ Ebner, G../Karsten, B./Lienemann, G./Wienroeder, M., Data Act, p. 97.
943 Grützmacher, M., *CR* 2024, 281 (292).

Art. 4(7) and (8) DA then provide for exceptions to this "fundamental priority of data access"[944] under strict conditions. The assertion of a right to refuse access is the *last resort* if the protection of trade secrets cannot be guaranteed in any other way.[945] If a data holder makes use of the grounds for refusal, the competent authority must be notified in accordance with both Art. 4(7) and Art. 4(8) DA. Art. 4(9)(a) and (b) DA give the user the opportunity to lodge a complaint with the competent authority against the refusal of the data holder or to refer the matter to a dispute resolution body pursuant to Art. 10(1) DA. The right to lodge a complaint is without prejudice to the user's right to appeal to a Member State court at any time, Art. 4(9) DA.

(1) Right of refusal pursuant to Art. 4(7) DA

According to Art. 4(7) DA, the data holder may refuse or suspend the disclosure of trade secrets if an agreement pursuant to Art. 4(6) DA is not reached, the user does not implement the agreed measures, or the confidentiality of the trade secrets is violated. The refusal or suspension must be duly justified, Art. 4(7) DA, which consequently requires a sufficiently concrete and case-specific justification.[946] The refusal or suspension of disclosure is also accompanied by an obligation on the part of the data holder to notify the competent authority, Art. 4(7)DA.

(2) Right of refusal pursuant to Art. 4(8) DA

Art. 4(8) DA also allows the data holder to refuse a data access request in individual cases for the specific data concerned if the disclosure is highly likely to cause serious economic damage to the data holder despite the measures set out in Art. 4(6) DA. This probability prognosis should be proven on the basis of objective facts and be sufficiently justified and communicated in writing to both the user and the competent supervisory authority (Art. 4(8) DA).

The DA does not define what exactly constitutes serious economic damage within the meaning of the standard. However, it follows from recital 31[947] that serious economic damage must be accompanied by irreparable economic losses. Demonstrating such damage in a forward-looking probability forecast in a sufficiently substantiated manner based on objective evidence is likely to pose considerable challenges for data owners on a regular basis. The extent to which Art. 4(8) DA therefore actually contributes to effective trade secret protection and the maintenance of investment incentives is doubtful due to these high requirements.[948]

bb) Disclosure of trade secrets to third parties, Art. 5 DA

The structure of Art. 5(9), (10), (11) DA is similar to that of Art. 4 Directive (EU) 2016/943 and regulates the disclosure of trade secrets to third parties.

944 Wiebe, A., *GRUR* 2023, 1569 (1573).
945 Andjic, M., *ZdiW* 2024, 68 (71).
946 Pauly, D./Wichert, F./Baumann, J., *MMR* 2024, 211 (213).
947 Rec. 31 Regulation (EU) 2023/2854.
948 Pauly, D./Wichert, F./Baumann, J., *MMR* 2024, 211 (213).

Pursuant to Art. 5(1) DA, the data holder must, at the request of a user, make readily available data and the metadata required for its use available to a third party. Paragraphs 9–11 DA limit this right with regard to accessing trade secrets.

(1) Restriction of data access by third parties pursuant to Art. 5(9) DA

Art. 5(9) DA provides for a restriction insofar as the disclosure must be absolutely necessary for the purpose agreed between the user and the third party. In order to protect the confidentiality of the disclosed data, data holder and third party, just like data holder and user in Art. 4(6) DA, should agree on appropriate technical and organisational measures. Prior to this, the affected business secrets of the data holder must be determined, Art. 5(9) DA.[949]

In the literature, the protection potential of the standard is questioned, as the data owner has no influence on the purpose agreed between the user and third parties.[950] According to the wording, any purpose could be agreed upon, which could then result in a disclosure obligation on the part of the data holder. In addition, artificially broad purpose agreements could be made from which a disclosure obligation could be derived. This harbours a considerable risk of abuse.[951]

The (limited) potential for protection arises primarily from the requirement that the disclosure must be absolutely necessary. A restrictive necessity standard – based on Art. 6(1)(b) GDPR – could limit the risks for data holders. In addition, a narrowly defined requirement of certainty with regard to the purpose agreement concluded between the user and the third party could prevent an improper and abusive extension of the agreed purpose.[952]

Nonetheless, a considerable risk remains, as even sufficiently specific purpose agreements can, under certain circumstances, give rise to very far-reaching access claims against which the DA does not provide any protective mechanisms.[953]

(2) Rights of refusal pursuant to Art. 5(10) and (11) DA

Paragraphs 10 and 11 of the Directive (EU) 2016/943 in turn provide for exceptions to the obligation of the data holder to disclose to third parties, which essentially correspond to the possibilities of refusal under Art. 4(7) and (8) DA vis-à-vis the user.[954] However, in order to prevent unauthorised disclosure and use by third parties, stricter measures will regularly be required to safeguard trade secrets. One

949 Raue, B., 'DA Art. 5', in: BeckOK Datenschutzrecht (49th ed. 2024) para 48.
950 Pauly, D./Wichert, F./Baumann, J., *MMR* 2024, 211 (214); Grapentin, S., *RDi* 2023, 173 (177); Metzger, A./Schweitzer, H., *ZEuP* 2023, 42 (75 et seq.).
951 Andjic, M., *ZdiW* 2024, 68 (72); Pauly, D./Wichert, F./Baumann, J., *MMR* 2024, 211 (214).
952 Pauly, D./Wichert, F./Baumann, J., *MMR* 2024, 211 (214).
953 Pauly, D./Wichert, F./Baumann, J., *MMR* 2024, 211 (215).
954 Rec. 31 of Regulation (EU) 2023/2854.

possibility in this regard is the use of **non-disclosure agreements** which, secured by contractual penalties, limit the third party's authorisation to disclose.[955]

cc) Summary

In view of the increasing relevance of data falling within the scope of the Directive (EU) 2016/943 and now simultaneously under that of the DA,[956] the relevance of the interplay between the two legal acts is also growing. It is striking that the DA clearly defines the relationship between access claims and trade secrets in favour of access. There is no comprehensive and effective trade secret protection in the DA in the event of a conflict.[957] The practical application of the DA remains to be seen in order to be able to assess the actual extent of the risk.[958]

To protect trade secrets, it is likely to be crucial for companies to prepare for the effects of the DA in practice and, in particular, to identify data as trade secrets in advance of any access requests pursuant to Art. 4(6) DA in order to be able to invoke the grounds for refusal under Art. 4(7) and (8) DA.[959] However, the identification of data as trade secrets is often a challenge in itself.[960] In view of the DA's far-reaching rights of access, however, this categorisation can be an important protection mechanism for trade secrets,[961] even if a right to refuse access only applies to correctly identified trade secrets.[962]

4. Summary and implications for practice

The relationship between the Data Act and the General Data Protection Regulation is characterised by numerous unresolved demarcation issues, which are often likely to lead to uncertainty in practice, which appears problematic, particularly in view of the parallel applicability of the fine provisions of the GDPR; unfortunately, the precedence clause of Art. 1(5) GDPR sheds little light on the matter. Companies therefore face the challenge of complying with the requirements of both regimes, which always requires a precise case-by-case examination of the data records to be made available. Under certain circumstances, the anonymisation of the relevant data can provide a remedy here.

In addition, the interaction of the Data Act with the Directive (EU) 2016/943 and the national implementing laws is becoming increasingly important, as the Data Act basically establishes the priority of data access over trade secrets without providing sufficient legal protection instruments in the event of a conflict. Companies should therefore check internally which data falls within the scope of the Data Act and at the same time affects trade secrets in order to be able to invoke the grounds for refusal of the DA if necessary.

---

955 Pauly, D./Wichert, F./Baumann, J., *MMR* 2024, 211 (215).
956 European Commission, Study on the legal protection of trade secrets in the context of the data economy - final report, 2022, p. 94.
957 Andjic, M., *ZdiW* 2024, 68 (73).
958 Andjic, M., *ZdiW* 2024, 68 (73).
959 Grützmacher, M., *CR* 2024, 281 (292).
960 Grützmacher, M., *CR* 2024, 281 (292).
961 Hennemann, M./Steinrötter, B., *NJW* 2024, 1 (4).
962 Raue, B., 'DA Art. 5', in: BeckOK Datenschutzrecht (49th ed. 2024) para 59.

III. Legal framework for data governance under the Data Governance Act (DGA) - Regulation (EU) 2022/868

Bibliography

Apel, S., & Huber, C., "Das neue Datenrecht der EU – Eine Übersicht," *JuS* (2024), 410; Bayerischer Landesbeauftragte für den Datenschutz, "Daten-Governance-Rechtsakt Auf dem Weg zu einem europäischen Binnenmarkt für Daten – Orientierungshilfe," accessible at: https://www.datenschutz-bayern.de/infothek/OH_DGA.pdf; Borges, G., & Keil, U. (eds.), Rechtshandbuch Big Data – Grundlagen, Rechtsfragen, Vertragspraxis, 1st ed., Nomos 2023; Bostelmann, K., Specht-Riemenschneider, L., & Hennemann, M., "Data Governance Act," *EuZW* (2024), 414; Brieske, J., Schweitzer, D., Müller, B., Pfeiffer, L., & Zihlmann, Z., "Zeitenwende beim Datenzugang? Struktur, Inhalte und Abstimmungsbedarf der aktuellen Regelungsvorschläge," *ZD-Aktuell* (2024), 04505; Brink, S., & Eckhardt, T., "Wann ist ein Datum ein personenbezogenes Datum? – Anwendungsbereich des Datenschutzrechts," *ZD* (2015), 205; von Ditfurth, L., "Datenmärkte, Datenintermediäre und der Data Governance Act – Eine Analyse der europäischen Regulierung von B2B-Datenvermittlungsdiensten," De Gruyter 2024; von Ditfurth, L., & Lienemann, G., "The Data Governance Act – Promoting or Restricting Data Intermediaries?" *CRNI* (2022), 270; Ehmann, E., & Selmayr, M. (eds.), Datenschutz-Grundverordnung, 3rd ed., 2024; European Commission, Commission staff working document impact assessment report accompanying the document Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), SWD(2020) 295 final; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Data Strategy, COM(2020) 66 final; European Commission, "Implementing the Data Governance Act – guidance document," accessible at: https://digital-strategy.ec.europa.eu/en/library/new-practical-guide-data-governance-act; Falkhofen, M., "Infrastrukturrecht des digitalen Raums," *EuZW* (2021), 787; Faustmann, T., "Der deliktische Datenschutz," *VuR* (2006), 260;
Gellert, R., & Graef, I., "The European Commission's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing," *TILEC Discussion Paper No. DP2021-006* (2021); von Hagen, P., & Völzmann, L., "Datenaltruismus aus datenschutzrechtlicher Perspektive – Wechselwirkung zwischen DGA und DS-GVO," *MMR* (2022), 176; Hartl, K., & Ludin, J., "Recht der Datenzugänge – Was die Datenstrategien der EU sowie der Bundesregierung für die Gesetzgebung erwarten lassen," *MMR* (2021), 534;
Hennemann, M., & von Ditfurth, L., "Datenintermediäre und Data Governance Act," *NJW* (2022), 1905;
Hoeren, T.,"Datenbesitz statt Dateneigentum – Erste Ansätze zur Neuausrichtung der Diskussion um die Zuordnung von Daten," *MMR* (2019), 5; Hornung, G., & Schomberg, A., "Datensouveränität im Spannungsfeld zwischen Datenschutz und Datennutzung: Das Beispiel des Data Governance Acts," *CR* (2022), 508; German Federal Ministry for Economic Affairs and Climate Protection, Vorläufige Stellungnahme zum Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance, accessible at: https://www.bmwk.de/Redaktion/DE/Downloads/S-T/stellungnahme-bundesrepublik-deutschland-zu-daten-governance-gesetz.pdf; Kühling, J., & Buchner, B. (eds.), DS-GVO, BDSG – Kommentar, 4th ed., C.H. Beck 2024; Kühling, J., & Schildbach, T., "Corona-Apps – Daten- und Grundrechtsschutz in Krisenzeiten," *NJW* (2020), 1545; Marx, S., "Verhaltenspflichten für Anbieter von Datenvermittlungsdiensten – Das Verhältnis zwischen DGA und DS-GVO," *ZD* (2023), 430;
OECD, Enhancing Access to and Sharing of Data – Reconciling Risks and Benefits for Data Re-Use Across Societies, 2019; Paschke, A., & Rücker, D. (eds.), Data Governance Act – Kommentar, 1st ed., C.H. Beck 2024; Picht, P., & Richter, H., "EU Digital Regulation 2022: Data Desiderata," *GRUR Int.* (2022), 395; Rachut, S., "Datenaltruismus unter dem Data Governance Act – Verpasste Chance

beim Zusammenspiel von DGA und DS-GVO," *ZD* (2024), 248; German Federal Ministry for Economic Affairs and Climate Protection, Referentenentwurf zur Durchführung der EU-Verordnung über europäische Daten-Governance (2024); Richter, H., "Ankunft im Post-Open-Data-Zeitalter – Datenwirtschaftsrecht II: Die Zukunft der Regulierung von Daten des öffentlichen Sektors," *ZD* (2022), 3; Richter, H., "Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine Verordnung über europäische Daten-Governance‘," *ZEuP* (2021), 634; Roßnagel, A., "Datenlöschung und Anonymisierung – Verhältnis der beiden Datenschutzinstrumente nach DS-GVO," *ZD* (2021), 188; Säcker, F.J., Rixecker, A., Oetker, H., & Limperg, S. (eds.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 9th ed., C.H. Beck 2021; Schildbach, T., "Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes," *ZD* (2022), 148; Schreiber, K., Pommerening, P., & Schoel, P., Das neue Recht der Daten-Governance – Data Governance-Act (DGA), 1st ed., Nomos 2023; Schreiber, K., & Schoel, P., "Data Governance Act: Mehr Daten für Legal Tech-Anwendungen?" *LTZ* (2024), 3; Schweitzer, H., "The Art to Make Gatekeeper Positions Contestable and the Challenge to Know What Is Fair: A Discussion of the Digital Markets Act Proposal," *ZEuP* (2021), 503; Simitis, S., Hornung, G., & Spiecker, I. (eds.), Datenschutzrecht – DS-GVO mit BDSG, 1st ed., Nomos 2019; Specht-Riemenschneider, L., "Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DS-GVO," *ZEuP* (2023), 638; Specht-Riemenschneider, L., & Blankertz, A., "Lösungsoption Datentreuhand: Datennutzbarkeit und Datenschutz zusammen denken," *MMR* (2021), 369; Specht, L., & Hennemann, M. (eds.), Data Governance Act – Handkommentar, 1st ed., Nomos 2023; Spindler, G., "Schritte zur europaweiten Datenwirtschaft – der Vorschlag einer Verordnung zur europäischen Daten-Governance," *CR* (2021), 98; Steinrötter, B., "Das Konzept einer datenaltruistischen Organisation," *DuD* (2021), 794; Steinrötter, B., "Datenaltruismus," *ZD* (2021), 61; Steinrötter, B. (eds.) , "Europäische Plattformregulierung," Nomos 2023; Sydow, G., & Marsch, N. (eds.), DS-GVO, BDSG – Handkommentar, 3rd ed., Nomos 2022; ; Taeger, J., & Gabel, D. (eds.), DS-GVO, BDSG, TTDSG – Kommentar, 4th ed., R&W Verlag 2022; Tolks, F., "Die finale Fassung des Data Governance Act: Erste Schritte in Richtung einer europäischen Datenwirtschaft," *MMR* (2022), 444; Weber, M., Rechtswörterbuch, 24th ed., C.H. Beck 2022; Wolff, H. A., Brink, S., & v. Ungern-Sternberg, A. (eds.), Beck’scher Online-Kommentar Datenschutzrecht, 49th ed., Status: 1 August 2024, C.H. Beck.

1. Introduction

Regulation EU 2022/868, known as the 'Data Governance Act' (DGA)[963], enriches data law as 'market design law' [964] with the structure of data governance. The law, which has largely been in force since 23 June 2023[965], is intended to break down data silos and establish an infrastructure for making data accessible.[966] The extent to which the Data Governance Act actually lives up to its claim of being a 'market

963 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (data governance act), OJ L 152, 3.6.2022, p. 1-44.

964 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed 2023, Introduction para. 5, 26; in agreement with Bostelmann, L., *EuZW* 2024, 414 (414); Specht-Riemenschneider, L., *ZEuP* 2023, 638¸ (641).

965 According to Art. 37 DGA, the obligations of the data exchange services, which are still to be described in more detail, are only binding from 24 September 2025.

966 Ehmann, E./Selmayr, M., Datenschutz-Grundverordnung, 3rd ed. 2024, Introduction para 136; Apel, S./Huber, C., *JuS* 2024, 410, (411).

design law' cannot yet be assessed.[967] What is certain, however, is that the DGA will not fit seamlessly into the existing European data protection regime.[968]

a) Problem analysis of the status quo

The EU Commission's problem analysis in the run-up to the DGA revealed that there is a low level of trust in the sharing of data in European society – and that there is not only a lack of clarity about the sharing of public data for the common good, but also technical hurdles that stand in the way of efficient data utilisation.[969] This has led to less data being shared than possible, which means that the economic and social potential of data is not being utilised. Estimates suggest that the increased sharing of company data could result in an overall European GDP increase of one to two and a half per cent.[970]

According to the Commission, the lack of data governance was problematic in four respects: firstly, some market power was consolidated in a few dominant companies such as *'Alphabet'*, *'Microsoft'*, *'Meta'* and *'Apple'*, which distorted competition on the data market and made it difficult for start-ups to enter the market because prohibitively high transaction costs had to be incurred to access and use data.[971] At the same time, the few companies that have been able to accumulate valuable data are likely to have been reluctant to share it for fear of losing their competitive advantage.[972] Secondly, all too much of the existing data would remain unused. According to the Commission, this data is missing from services that could already be better today with its help. It would not be used to drive innovation (such as data training for AI) and would also take momentum away from the European labour market, which could benefit from a flourishing data economy.[973] Thirdly, the internal market is fragmented in regulatory terms with regard to data. A common harmonised market for data is also important in order to drive inter-European innovation.[974] And fourthly, the status quo has meant that the EU has become dependent on third countries (probably meaning the USA) in promising sectors, particularly data-driven business models. The innovation taking place there in particular could even lead to a 'brain drain', i.e. the emigration of European data experts.[975]

The EU Commission's problem analysis clearly shows that European legislators are also concerned about geopolitical issues such as the DGA, i.e. being left behind socially and economically in the face

967 For an overview of the criticism of the DGA, see Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 115 et seq.
968 On the relationship between the DGA and data protection law, see Paschke, A./Rücker, D., DGA, 1st ed. 2023, Introduction, para. 38 et seq.
969 Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1906); SWD(2020) 295 final, p. 8, 15.
970 OECD, Enhancing Access to and Sharing of Data, 2019, p. 11, 62 et seqq; SWD(2020) 295 final, p. 9.
971 SWD(2020) 295 final, p. 8.
972 Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1906).
973 SWD(2020) 295 final, p. 8.
974 SWD(2020) 295 final, p. 17 et seq.
975 SWD(2020) 295 final, p. 8.

of rapid technological change without efficient data utilisation.[976] Seen in this context, the DGA represents a move in the 'competetion of regimes', in which the EU is trying to position itself as a player on an equal footing with China and the USA.[977]

b) Importance and function of data governance

The DGA is a fundamental or introductory part of the EU Commission's **data strategy**. The first proposal for a regulation was issued in 2020.[978] The DGA is intended to establish **'data governance'** as a structuring element of the data economy. The term 'data governance' refers to a system for regulating and organising the handling of data.[979] Specifically, the term data governance can be defined as a comprehensive data-related view of technology, economics, society, politics and regulation.[980] According to this definition, data is a "raw material" that assumes a different value in different "data ecosystems" depending on the context and "knowledge objective". The task of data governance is therefore to incentivise the responsible use and sharing of data while at the same time defining the limits and conditions of data exchange.[981]

The main objective of the DGA is the development of a border-free internal market[982] , particularly with regard to the data economy.[983] The DGA – like all legal acts of the 2020 data strategy – is intended to avoid regulatory fragmentation of the digital areas of individual sectors.[984] In addition to the development of the internal market, the aim is also to ensure that EU citizens benefit from a trustworthy and secure data society and economy.[985]

Overall, the DGA aims to lower the inhibition threshold for individuals and companies to share their data with the general public.[986] It also aims to break the market power of big tech companies, which have a large amount of data at their disposal due to their dominant position, by giving smaller companies access to large amounts of data.[987] One of the aims of the DGA is therefore to utilise the potential of data sharing.[988]

---

976 Specht-Riemenschneider, L./Hennemann, M., HK-DGA, 1st ed, Introduction para. 16.
977 Specht-Riemenschneider, L./Hennemann, M., HK-DGA, 1st ed, Introduction para. 17.
978 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 1 para. 4.
979 Paschke, A./Rücker, D., DGA, 1st ed. 2024, Introduction, para. 6; Schreiber/Pommerening/Schoel, Das neue Recht der Daten-Governance, 2023, § 1 para. 3.
980 Specht-Riemenschneider, L./Hennemann, M., HK-DGA, 1st ed. 2023, Introduction para. 1.
981 Specht-Riemenschneider, L./Hennemann, M., HK-DGA, 1st ed. 2023, Introduction para. 1-3.
982 Rec. 3 Regulation (EU) 2022/868; Paschke, A./Rücker, D., DGA, 1st ed. 2024, Introduction, para. 6.
983 Tolks, D., *MMR* 2022, 444, (448).
984 COM(2020) 66 final, p. 14.
985 Rec. 5 Regulation (EU) 2022/868; COM(2020) 66 final, p. 5.
986 Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1907).
987 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1907).
988 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 1 para. 4; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1905).

In terms of the legal system, the DGA is a hybrid and does not fit easily into the traditional threefold division of the German legal system, as it attempts to take into account the complexity of data use in both social and economic terms and addresses not only public authorities and private individuals, but also companies that are commercially active.[989] The form of regulation with which the EU wishes to pursue data governance via the DGA is commonly referred to as 'market design'[990].

Specifically, the DGA initially aims to achieve trust in the sharing of data among the addressees. This is to be achieved in particular through the provisions of Chapters 3 and 4.[991] At the same time, the DGA is intended to establish the legal infrastructure for data sharing, with Chapters 2 and 4 playing a special role here.[992] Finally, with the provisions of Art. 16-25 (Chapter 4), the DGA is also intended to promote the altruistic disclosure of data in the public interest.[993]

The meaning of the DGA is summarised in recital 3. The DGA is a horizontal regulation for the re-use of certain categories of protected data held by public sector bodies and for the provision of data intermediary services and services based on data altruism within the EU.[994]

c) Principles and systematics of the DGA

In the first chapter, the DGA defines its subject matter and scope as well as all relevant definitions. The relevant provisions of the DGA can be divided into the following three areas:

1. Re-use of data held by public sector bodies (Art. 3–9 DGA)
2. Provision and use of data intermediation services (Art. 10–15 DGA)
3. Data altruism (Art. 16–25 DGA)

The second chapter of the DGA is dedicated to the **re-use of data held by public sector bodies**. According to the legislator, data generated or collected with the help of public funds should be reused and benefit the general public.[995] However, no entitlements to re-use are granted here, but rather the conditions for which data can be accessed, how and by whom.

The third chapter then establishes regulations for a new player on the data economy market: **data intermediation services**. The new legal services brought onto the scene by the DGA are intended to enter the data market as neutral third parties. Data intermediation services are intended to bring individuals and companies together with data users in order to create business relationships.[996] In other words, data intermediation services have a transaction cost-reducing bridging function between those who have data

989 Specht-Riemenschneider, L./Hennemann, M., HK-DGA, 1st ed. 2023, Introduction para. 5.
990 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 5.
991 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 41-42.
992 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 46.
993 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 50.
994 Rec. 3 Regulation (EU) 2022/868.
995 Rec. 6 Regulation (EU) 2022/868.
996 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.

and those who need data by collecting the data to be shared in trust and making it accessible.[997] Since data intermediation services are a data economy actor created by the DGA, the obligations of Chapter 3 in this regard pursuant to Art. 37 DGA are only mandatory from 24 September 2025, provided that the data intermediation services referred to in Art. 10 DGA were already provided by the entity before 23 June 2022. If, on the other hand, an organisation provides the data intermediation services referred to in Art. 10 DGA for the first time after 23 June 2022, the obligations of Chapter 3 apply immediately. There is no transitional provision.

In the fourth chapter, the DGA introduces the constellations of **data altruism**. According to the legislator, data is made accessible and reused on a voluntary basis without commercial interest.[998] In cases of data altruism, no payment is made in return; access is granted for the public good.

The fifth chapter lays down rules to be complied with by the national authorities monitoring compliance with the DGA and provides data subjects with a right of appeal and a right to an effective judicial remedy. The **European Data Innovation Board** is introduced as a new institution in the sixth chapter. Its main task will be to advise and support the Commission in the development of standardised practices and guidelines in relation to data governance.[999] Finally, the seventh chapter regulates the international application of the DGA, the eighth chapter authorises the Commission to adopt its own legal acts and the ninth chapter provides for the final provisions, in particular possible sanctions.

The structure of this chapter is also based on this system specified by the DGA. Firstly, the regulations for data held by public sector bodies are discussed (3.). This is followed by a presentation of data intermediation services (4.) and data altruism (5.).

d) Demarcation of the DGA from the GDPR

In order to understand the DGA as part of the EU Commission's comprehensive data strategy, it must be read in conjunction with other legal acts of digital law.[1000] Of particular importance here is the relationship and demarcation between the DGA and the GDPR[1001]. The DGA leads to a not insignificant expansion of the processing of data, including personal data, so that there is a partial overlap between the areas of the DGA and the GDPR.[1002]

997 SWD(2020) 295 final, p. 12; Hennemann, M./von Ditfurth, L., *NJW* 2022, 1905, (1906); see with further references Tolks, D., *MMR* 2022, 444, (446).

998 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 68.

999 Paschke, A,/Rücker, D./Keppeler, L./Poncza, H., DGA, 1st ed. 2024, Art. 29 para. 6.

1000 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 37.

1001 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1-88.

1002 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 1 para. 23.

In addition to the GDPR, the DGA must also be seen in the context of the Free Flow of Data Regulation[1003], the PSI Directive[1004] and the Directive (EU) 2016/943[1005]. In particular, the DGA should also correspond with the other legal acts of the data strategy, especially DA[1006], DSA[1007] and DMA.[1008]

aa) Legal requirements for demarcation

For the DGA – as for many Union legal acts – the "primacy of non-prejudice" applies with regard to the demarcation from the GDPR[1009] (Art. 1(3) DGA).[1010] As a result, the GDPR only takes precedence in the event of a conflict.[1011] However, the DGA contains numerous provisions on the utilisation of data that are in conflict with the GDPR. The legislative paradigm shift from data protection to data utilisation is evident in the DGA in that the legal act fundamentally deals with the shared use of data without distinguishing between personal and non-personal data at the outset.[1012] This means that the objectives of the EU data protection regime that has applied to date and continues to apply and those of the DGA (and data law as a whole) are more or less in conflict with each other.[1013] The consequence is that the blanket statement in Art. 1(3) DGA, according to which the GDPR remains unaffected, does not lead to a resolution of the tension. Instead, regulatory and conceptual questions of priority and demarcation arise in individual cases.[1014]

The widespread view in the literature is that the DGA should be interpreted and read with regard to its scope in such a way that its provisions do not come into conflict with the GDPR. If they do, which is regularly the case for personal data, the GDPR takes precedence.[1015]

In unclear situations, the first key question is therefore whether the facts of the case bring two provisions of the GDPR and the DGA into conflict. If, on the other hand, a 'cooperation relationship'[1016] can be

---

1003 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on on a framework for the free flow of non-personal data in the European Union, OJ L 305, 28.11.2018, pp. 59-68.

1004 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, pp. 56-83.

1005 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, pp. 1-18.

1006 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules for fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, OJ L, 22.12.2023, pp. 1-71.

1007 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC, OJ L 277, 27.10.2022, pp. 1-102.

1008 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ L 265, 12.10.2022, pp. 1-66.

1009 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 87.

1010 The aim of the legislator has been to strengthen the provisions of the GDPR, cf. European Commission, Implementation of the DGA Guidelines, p. 2.

1011 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.

1012 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 37.

1013 Cf. Tolks, D., *MMR* 2022, 444, (444) on fears in the context of the resolution procedure.

1014 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 8.

1015 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 89; Marx, S., *ZD* 2023, 430, (431); Rachut, S., *ZD* 2024, 248, (250).

1016 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 92.

created between two standards, for example by applying an opening clause of the GDPR, the question of demarcation does not arise. Taking into account recent ECJ case law[1017] on the conflict of EU law standards, it can be concluded that the DGA only takes a back seat to the GDPR in two cases: firstly, if the DGA imposes less stringent requirements on the GDPR without the GDPR being open to a derogation and, secondly, if the DGA imposes a completely different requirement on data processing and the provisions of the GDPR are waived in the process without there being an opening clause.[1018]

bb) Criticism

However, this abstract rule rarely solves practical details: The fact that the DGA and the GDPR are based on a partially inconsistent vocabulary and that there are open contradictions in terms of protective measures such as anonymisation can cause difficulties in individual cases.[1019] The inconsistency is also reflected in the language and concepts: while the GDPR categorises data subjects, controllers, processors and recipients, the DGA refers to **data holders, data users and data intermediaries**. It may not always be immediately clear to whom which roles and obligations can be clearly and practicably assigned in cases of conflict.[1020]

The fact that the relationship between the DGA and the GDPR is unclear from the outset is already evident from the definition of 'data': In principle, Art. 2 No. 1 DGA conclusively defines the term "data" as any digital representation of actions, facts or information and any compilation of such actions, facts or information, including in the form of sound, visual or audiovisual material. For the term personal data, however, Art. 2 No. 3 DGA refers to the GDPR, which according to Art. 4 No. 1 GDPR also covers analogue information in principle.[1021] The question therefore arises as to whether or not this analogue data is also covered by the DGA.[1022] Another question of priority and demarcation that has not been clarified by the legislator is what is meant by the term consent in the context of Art. 12 (e) DGA. The fact that Art. 2 No. 5 DGA legally defines consent and that it is only explicitly mentioned in Art. 12 (m), (n) DGA speaks against the assumption that this is consent in accordance with Art. 4 No. 11 GDPR.[1023]

In addition to the technical demarcation issues, the primacy of non-discrimination also means an immense reduction in effectiveness if the innovation standard of the data strategy envisaged by the Commission is applied: This is because every data intermediation service – actually intended as the novelty for establishing **agile data transfer** – must check each data set to be brokered for personal data on a case-by-case basis.[1024] This is an immense amount of work, which in terms of innovation probably only

---

1017 See for example CJEU, 13 Sept. 2018, case - C-54/17, C-55/17, EU:C:2018:710, para. 60 - Wind Tre.
1018 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 92.
1019 Brieske, J./Müller, B./Pfeiffer, L./Zihlmann, Z., *ZD-Aktuell* 2024, 04505; Marx, S., *ZD* 2023, 430, (431).
1020 Marx, S., *ZD* 2023, 430, (431) et seq.
1021 Taeger, J./Gabel, D./Arning, M./Rothkegel, T., GDPR - BDSG - TTDSG, 4th ed. 2022, Art. 4(7).
1022 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 1 para 27; Marx, S., *ZD* 2023, 430, (431).
1023 Marx, S., *ZD* 2023, 430, (433); regarding further individual delimitation difficulties see Tolks, D., *MMR* 2022, 444, (448) et seq.
1024 Marx, S., *ZD* 2023, 430, (44).

differs from the status quo in that it takes place at a newly created location. Furthermore, if the personal information is relevant to competition, the level of protection of the GDPR is even exceeded. According to Art. 12(l) GDPR, the provider must ensure the highest level of security, whereas according to Art. 32(1), of the GDPR, there is only an obligation to take appropriate technical and organisational measures to protect personal data.[1025] It is not clear which measures can fulfil the highest level of security. If the best conceivable protection is actually owed, this is likely to overburden most providers both technically and financially.[1026]

2. Data held by public sector bodies, Art. 3–9 DGA

Chapter 2 of the DGA regulates the Re-use of certain categories of protected data held by public sector bodies.

a) Sense and purpose of the regulations

The DGA establishes conditions for the transfer of data held by public sector bodies, Art. 1(1) DGA.

Against this background, the first question that arises is why **public bodies** in particular are addressed by the DGA in Chapter 2. One of the main aims of the DGA is to make data financed from public funds accessible.[1027] As part of this, administrative data from public bodies is to be made available to the general public for non-governmental purposes.[1028] The term 'non-governmental-purposes' is understood to mean a purpose that benefits the common good, whereby the common good is decisive.[1029] The reuse of data is seen as an opportunity to establish new business models or to make a valuable contribution to public services of general interest.[1030]

If data held by public sector bodies were not covered by the DGA, some fear that de facto barriers to the use of data could arise because the data sets held by public sector bodies are particularly large. [1031] However, the purpose of the DGA is precisely to create a common use of data in the internal market and a harmonised legal framework for data exchange[1032] in order to fully exploit the potential that lies in the use of data. It is clear that this potential can only be realised if as much data as possible is included in the regulations of the DGA – including the many data held by public sector bodies.

1025 Cf. also Rachut, S., *ZD* 2024, 248, (252); Marx, S., *ZD* 2023, 430, (433).
1026 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 3 para. 113 et seq.; Marx, S., *ZD* 2023, 430, (433).
1027 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 2 para. 1.
1028 Rec. 6 Regulation (EU) 2022/868.
1029 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 3 para. 11.
1030 Falkhofen, B., *EuZW* 2021, 787, (789).
1031 Wischmeyer, T., 'DGA Art. 3', in: BeckOK Datenschutzrecht (49th ed. 2024) para 6.
1032 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 1 para. 3.

The provisions of the DGA are thus part of the European regulation of the disclosure of public sector data, which began with the PSI Directive.[1033] The aim of the DGA is precisely to compensate for the weaknesses of the PSI Directive, as the PSI Directive only regulated the re-use of publicly accessible information held by the public sector bodies that can be passed on without specific restrictions or limitations. In the case of databases containing personal data or confidential business information, this meant that disclosure as public data was only possible if it was anonymised or aggregated so that no potential re-user could re-identify individuals or confidential information.[1034]

b) Addressees of the provisions of the second chapter

The second chapter of the DGA deals with the Re-use of certain categories of protected data held by public sector bodies, Art. 3(1) DGA. The exact addressees and subjects of the chapter are defined in the definition section (Art. 2 DGA). Some of the definitions were taken from the Open Data Directive, which in turn draws its terminology from the EU Public Procurement Directives.[1035]

The term public bodies is legally standardised in Art. 2 No. 17 DGA. According to Art. 2 No. 17 DGA, **public sector bodies** are the state, regional or local authorities, bodies governed by public law or associations formed of one or more of these bodies or one or more of these bodies governed by public law. This definition has been adopted from No. 11 of the draft regulation without any change in content.[1036]

In addition, the provisions of the second chapter also cover so-called **bodies governed by public law**[1037], which are described in more detail in Art. 2 No. 18 DGA. Accordingly, an body governed by public law exists if it cumulatively performs a task in the public interest (a) and has a legal personality (b) as well as a 'special state link '[1038] in the sense of predominantly state funding (c).

Furthermore, Art. 3(2) DGA specifies to which addressees the provisions of the second chapter do not apply by way of exception, although they are actually public bodies.

The first exception applies to **public undertakings** pursuant to Art. 3(2) DGA. According to Art. 2 No. 19 DGA, a public undertaking is one over which public sector bodies may exercise directly or indirectly a dominant influence by virtue of their ownership, their financial participation or the provisions applicable to the undertaking. The emphasis here is particularly on the criterion of dominant influence. In order to concretise this criterion, No. 19 (a–c) DGA provides examples of cases in which such a dominant influence is undoubtedly present.[1039]

[1033] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56-83.
[1034] European Commission, Implementation of the DGA - Guidelines, p. 3.
[1035] Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 2 para. 8.
[1036] Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 24.
[1037] Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 2 para. 7.
[1038] Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 2 para. 8.
[1039] Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 2 para. 153.

According to Art. 3(2) DGA, the second chapter also does not apply to **public service broadcasters**. Accordingly, organisations and their subsidiaries are exempt from complying with the provisions of Chapter 2 of the DGA for such data that serve to fulfil a public broadcasting mandate.[1040]

Finally, Art. 3(2) DGA also excludes cultural and educational institutions from its scope . According to recital 12 of the DGA, these include libraries, museums, operas, universities and schools.[1041] The rationale behind these exceptions is that the rights of third parties in the form of intellectual property rights are often affected in these institutions.[1042] If one of the exceptions applies, Art. 4 et seq. DGA are therefore not applicable.

c) No obligation of public sector bodies to disclose, Art. 1(2) DGA

Contrary to what the unofficial title might suggest, Art. 1(2) DGA does not impose an obligation on public bodies to authorise the re-use of data, meaning that any access rights to certain datasets or documents continue to be governed exclusively by national law.[1043] Art. 1(2) DGA thus makes it clear that the DGA – unlike the Data Act – does not establish data access rights or disclosure obligations for documents; rather, this regulation is about creating a functioning data utilisation infrastructure.[1044] This in turn is clear from recital 11. In particular, the DGA does not constitute a new legal basis within the meaning of the GDPR for the re-use of personal data.[1045]

Furthermore, the DGA does not exempt public bodies from their confidentiality obligations under Union or national law. The DGA does not provide a definition of the term 'confidentiality obligations'; however, it is evident that both statutory and contractual confidentiality obligations will be covered.[1046] These are likely to include not least commercial confidentiality obligations to protect intellectual property, but also statutory confidentiality obligations such as tax confidentiality[1047]. As a result, the DGA does not contain any exceptions or other authorisations.

In view of the fact that public bodies are not obliged to provide data, the question arises as to how exactly this aspect should be categorised in relation to the judicially enforceable requests for re-use, which are regulated in Art. 9(1) DGA.[1048] More detailed explanations from the Commission would have been desirable here.

1040 Wischmeyer, T., 'DGA Art. 3', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 26.
1041 Rec. 12 Regulation (EU) 2022/868.
1042 Rec. 12 Regulation (EU) 2022/868; Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 2 para. 22.
1043 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 2 para. 2; Tolks, D., *MMR* 2022, 444.
1044 Rec. 12 Regulation (EU) 2022/868; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 1 para. 32.
1045 European Commission, Implementation of the DGA - Guidelines, p. 3 et seq.
1046 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 1 para. 37.
1047 Cf.: Section 30 of the German Fiscal Code (AO) stipulates the confidentiality obligation for national law.
1048 https://www.bmwk.de/Redaktion/DE/Downloads/S-T/stellungnahme-bundesrepublik-deutschland-zu-daten-governance-gesetz.pdf?__blob=publicationFile&v=4 .

d) Objectively recorded data and actions, Art. 3(1) DGA

According to Art. 3(1) DGA, the second chapter regulates the re-use of data which is in the possession of public sector bodies and are protected according to certain criteria.

aa) Re-use of the data

Before discussing the different categories of data in Art. 3(1), the term **"re-use"**, which is central to the second chapter, must first be clarified.

According to Art. 2 No. 2 DGA, re-use means the use of data by natural or legal persons for commercial or non-commercial purposes other than the original purpose in the context of the public task for which the data were collected. The term "re-use" within the meaning of the DGA is therefore very similar to the term "further processing" within the meaning of Art. 6(4) GDPR.[1049] In both cases, the original purpose of the data collection differs from the purpose of the re-use of the data that is now being pursued. The only decisive factor here is that the purpose of the re-use is different from the purpose originally pursued by the public sector body.[1050] However, only non-governmental purposes are covered, which is why there is no re-use if public bodies exchange their data exclusively in the context of fulfilling their public mandate.[1051] Furthermore, the concept of re-use is linked to the concept of utilisation, whereby utilisation is not defined in more detail by the DGA.[1052] Due to this lack of concretisation, a broad interpretation of the concept of use is likely to be required.[1053]

bb) Data held by public sector bodies

In addition to re-use, it also depends on whether the **data** is also **held by** the public sector bodies. When exactly data is in the possession of public sector bodies is not further defined in the DGA. According to one view in the literature, the wording of the definition of possession suggests that, based on Section 854 of the German Civil Code (BGB), actual control over the data must be assumed in order to speak of possession.[1054] This means that if a public body can de facto determine the possible use of the data, it is in possession of the data.[1055] According to § 854 BGB, in contrast to ownership, possession depends on the actual control of a thing, but not on the legal control.[1056]

Others, however, do not refer to § 854 BGB, but argue that the term "in possession" must rather be interpreted in accordance with EU law.[1057] One argument in favour of this is that many EU member states do not recognise the German understanding under civil law, according to which possession is

1049 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 5 para. 36.
1050 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 5 para. 37.
1051 Schreiber K./Schoel P., *LTZ* 2024, 3 (5).
1052 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 39.
1053 Paschke, A,/Rücker, D./Keppeler, L./Poncza, H., DGA, 1st ed. 2024, Art. 2 para. 7.
1054 Paschke, A,/Rücker, D./Keppeler, L./Poncza, H., DGA, 1st ed. 2024, Art. 2 para. 8.
1055 Paschke, A,/Rücker, D./Keppeler, L./Poncza, H., DGA, 1st ed. 2024, Art. 2 para. 8.
1056 Hoeren, T., *MMR* 2019, 5 (6).
1057 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 37.

linked to the principle of abstraction, in our form.[1058] Therefore, it depends on its understanding as a technical-factual data dominion, which is characterised by an actual possibility of influencing the data.[1059] The English version, which speaks of "data held by public sector", also speaks in favour of this standard.[1060] Ultimately, however, both justifications will probably come to the same conclusion in most cases, as Section 854 BGB is also based on de facto control.[1061]

However, if you want to be sure, it is advisable to interpret the term "in possession" in accordance with Art. 2 No. 2 DGA under EU law and to subsume it accordingly.

According to the literature, the "material control" of the data at the time of their creation (generation) is not relevant for the applicability of Art. 3 DGA.[1062]

cc) Specially protected data

Chapter II of the DGA applies pursuant to Art. 3(1)(a)–(d) DGA to certain specially protected data, which are explained in more detail below:

(1) First data group: Commercial confidentiality to Art. 3(1)(a) DGA

This refers to all data that describes the "circumstances of private third parties, usually legal entities" that "must be treated confidentially", i.e. in any case all information that would also constitute a trade secret within the meaning of the GeschGehG.[1063] A **trade secret**, in turn, is any information that is not readily accessible, not generally known and therefore of commercial value. The data is protected by its owner through confidentiality measures, as the owner has a legitimate interest in maintaining confidentiality.[1064]

The concept of commercial confidentiality also includes trade secrets, professional secrets and business secrets, as defined in Art. 3(1)(a) DGA.

(2) Second data group: Statistical confidentiality pursuant to Art. 3(1)(b) DGA

In addition, according to Art. 3(b) DGA, data that is protected for reasons of **statistical confidentiality** are covered by Chapter 2. This refers to confidential data that is protected under primary law by Art. 339(2) TFEU and more precisely by the Statistics Regulation (EC 223/2009).[1065] Data of statistical confidentiality refers to data that may be used about certain persons or companies, whereby regulations

---

1058 Paschke, A./Rücker, D., DGA, 1st ed. 2024, Art. 2 para. 8.
1059 Schild, H./Richter, H./Schmidt-Wudy, F., 'DGA Art. 2', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 27; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 37.
1060 Paschke, A./ Rücker, D., DGA, 1st ed. 2024, Art. 2 para. 8.
1061 Schild, H./Richter, H./Schmidt-Wudy, F., 'DGA Art. 2', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 27.
1062 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 37.
1063 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 28.
1064 Cf. Art. 2 No. 1(a) – (c) Trade Secrets Directive.
1065 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 31.

must be applied to prevent the disclosure of this data.[1066] Statistical confidentiality protection is enshrined in law at national and EU level, in particular through the Statistics Regulation[1067].[1068]

(3) Third data group: Intellectual property pursuant to Art. 3(1)(c) DGA

According to Art. 3(1)(c) DGA, Chapter 2 also applies to data held by public sector bodies which is protected for reasons of intellectual property rights of third parties. Art. 3(1)(c) DGA is a reference to the European and national provisions of copyright law. It is true that the DGA is also intended to create accessibility to such data that is relevant under copyright law. However, the DGA does not constitute an exception to the validity of existing copyright law. Accessibility of specially protected data in accordance with Art. 3(1)(c) DGA can therefore only take place if the corresponding copyright regulations are complied with.[1069] In the course of this, the copyright-protected database work, the database producer's right and the protection under patent law will be of particular importance.[1070]

(4) Fourth data group: Protection of personal data pursuant to Art. 3(1)(d) DGA

As a fourth and final group, Art. 3 also refers to specially protected personal data, Art. 3(1)(d) DGA. The concept of personal data is to be equated with that of Art. 4 No. 1 GDPR. Accordingly, personal data is any information relating to an identified or identifiable natural person. However, data that falls within the scope of the PSI Directive is no longer covered. As a result, the DGA only applies in these cases on a subsidiary basis.[1071] Specifically, Art. 3(1)(d) DGA is linked to Art. 1(2)(h) PSI Directive. This in turn excludes the application of the Directive to documents that are not accessible or only accessible to a limited extent under the access regulations of the Member States for reasons of personal data protection and parts of documents that are accessible under these regulations if they contain personal data whose re-use is legally incompatible with the law on the protection of natural persons with regard to the processing of personal data or is legally defined as compromising the protection of the privacy and integrity of the data subjects, in particular in accordance with Union law or national law with regard to the protection of personal data. Since it is precisely these personal data that are not regulated by the PSI Directive, the application of the DGA extends to these data in particular.[1072]

Art. 2 No. 6 DGA defines the requirements for a document within the meaning of the PSI Directive: Document means any content irrespective of the form of the data carrier or any part of such content.

1066 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 3 para. 30.

1067 Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities, *OJ L 87, 31.3.2009, p. 164-173*.

1068 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 3 para. 30.

1069 Rec. 17, 18 Regulation (EU) 2022/868; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 32.

1070 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 3 para 32; otherwise Wischmeyer, T., 'DGA Art. 3', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 19.

1071 Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 3 para. 26.

1072 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 3 para. 41.

e) Exclusion of certain types of data in Art. 3(2)(d),(e) DGA

As outlined above, the exceptions in Chapter 2 apply to various types of institutions that hold the protected data and should normally be categorised as public bodies, Art. 3(2)(a)–(d) DGA. If such an institution exists, such as a public company, museums, schools and universities, the provisions of Chapter 2 DGA are not applicable.[1073] In addition, certain types of data in Art. 3(2)(d) and e) DGA are also covered by the derogation, which is not linked to the owner of the data but is based on the quality of the data.[1074] This includes data that may not be shared for reasons of national security/defence or public security (d), as well as data that is not collected within the statutory mandate of the public sector body (e). With regard to the first group, it should be noted that this exception is intended to take account of the limited competence of the European Union in these matters.[1075] The competent authority itself will have to assess which data exactly falls under the concept of public security, as the provision on "public security" is subject to interpretation and cannot be assessed uniformly in all Member States.[1076] With regard to the second group of exceptions, such a public task may arise from the general administrative practice of the respective Member State; this must be transparent and regularly reviewed.[1077]

f) Prohibition of exclusive arrangements, Art. 4 DGA

According to Art. 4(1) DGA, it is generally prohibited to conclude an **exclusive arrangements** with regard to re-utilisation. According to Art. 4(1) DGA, exclusive arrangements are agreements or other practices which grant exclusive rights or which have as their object or effect the granting of such exclusive rights. Agreements are to be understood as any form of contractual obligation, while other practices represent a kind of catch-all provision that is intended to exclude an immediate telos outside the characteristics of an agreement. Agreements are voluntary agreements; other practices, on the other hand, are also intended to cover other forms of action, such as administrative acts.[1078] If an administrative act exists, it is not only ineffective but also void.[1079] The addition of other agreements is intended to prevent circumvention.[1080]

The very broad prohibition of exclusive arrangements ensures that both direct and indirect restrictions on third-party access to data held by public sector bodies for re-use are prevented through agreements or other practices.[1081] A violation of Art. 4(1) DGA may have a negative impact on the effectiveness of the corresponding agreement.[1082]

1073 European Commission, Implementation of the DGA - Guidelines, p. 4.
1074 Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 3 para. 61.
1075 Wischmeyer, T., 'DGA Art. 3', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 29.
1076 Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 3 para. 62.
1077 Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 3 para. 63.
1078 Richter, H., 'DGA Art. 4', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 6.
1079 Richter, H., 'DGA Art. 4', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 14.
1080 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 44 - 49.
1081 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 4 para.34.
1082 Richter, H., *ZD* 2022, 3 (5).

The overall aim of this provision is that data from public bodies should be available to everyone as far as possible in order to maximise the degree of innovation.[1083]

Art. 4(2) DGA establishes an exception to the fundamental prohibition of exclusive agreements, under the conditions of which an exclusive agreement is permissible: Accordingly, an exclusive agreement may be concluded between a public body and a third party if the provision of a service or product in the **general interest** would otherwise not be possible. The open term "general interest" must be interpreted autonomously under EU law.[1084] In any case, it should not include only private, individual concerns of the individual; rather, it should be about concerns that affect a large number of people. For example, healthcare, improving the provision of public services or combating climate change are in the general interest.[1085] Recital 13 can also be used as a guide, which cites the provision of a product (e.g. the manufacture of a medicine) as an example of a general interest.[1086] However, this must be justified in a sufficiently transparent manner (5) and be legally effective through an administrative act or contractual agreement (3). Furthermore, such an exclusivity agreement may not exceed a duration of 12 months (4). These substantive, formal and procedural requirements of (2)–(5) must be met cumulatively.[1087]

g) Conditions for re-use, Art. 5 DGA

Art. 5 DGA is the central component of the DGA and standardises the conditions under which re-use is permitted. According to Art. 5(2) DGA, the basic principle is that the conditions for re-use must be non-discriminatory, transparent, proportionate and objectively justified.

The conditions for authorising the re-use of specially protected data and the procedure for requesting such re-use must be made publicly accessible via the central information point (Art. 8 DGA), Art. 5(1) DGA. Interested companies and other data users will only benefit from data access claims if they can find out in a transparent and legally secure manner under what conditions they can access the data.[1088] With this in mind, it is recommended that public bodies use a standardised confidentiality obligation and also inform re-users of their obligations by means of standardised information within the framework of Art. 5(1) DGA; if necessary, this should also be provided in a separate portal on their website.[1089]

1083 Richter, H., 'DGA Art. 4', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 2; Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 3 para. 1.

1084 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 4 para. 57.

1085 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 4 para. 57.

1086 Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 4 para. 9 et seq.

1087 Richter, H., 'DGA Art. 4', in: BeckOK Datenschutzrecht (49th ed. 2024) para 1.

1088 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 64.

1089 The Bavarian State Commissioner for Data Protection, Data Governance Act Towards a European Single Market for Data - Guidance, para. 46, https://www.datenschutz-bayern.de/infothek/OH_DGA.pdf (last accessed on: 1 November 2024).

Art. 5(3)–(14) DGA sets out the individual requirements and conditions for re-use, whereby the protection of data always has the highest priority, regardless of whether it is personal or non-personal data.[1090] Differences exist only with regard to the specific measures taken to protect the data.

aa) Protective measures for personal data

According to the legislator, the protection of personal data is achieved by anonymising it, Art. 5(3)(a) point i DGA. The specific wording of this provision does not establish anonymisation as an official obligation; rather, it is presented as one among a range of potential methods.[1091] In this context, the question known from data protection law as to when anonymisation is to be assumed becomes relevant. According to recital 26 GDPR, data is anonymous if it does not relate to an identified or identifiable natural person or if it is personal data that has been anonymised in such a way that the data subject cannot or can no longer be identified.[1092] According to recital 26 GDPR, when deciding whether identifiability is possible, all means that are likely to be used by the controller or another person to directly or indirectly identify the natural person must be taken into account.[1093] However, it should be noted that a fictitious possibility of identifiability is not sufficient.[1094] Instead, in the opinion of the European Court of Justice, those means by which identification would not be practically feasible, for example because they would require a disproportionate amount of time, cost and labour, are not to be taken into account.[1095] However, it is disputed whether and, if so, to what extent the knowledge and means of other persons can be taken into account to identify a person. The question is therefore whether the ability to establish a personal reference depends on the person responsible (relative personal reference)[1096] or whether it is sufficient if any other person can establish a personal reference (absolute personal reference).[1097] The European Court of Justice takes a mediating position on this issue. According to the court, it depends on whether the controller has means at his disposal that he can reasonably use to obtain the information from a third party.[1098]

1090 For a detailed overview of the obligations to be complied with, see European Commission, Implementation of the DGA - Guidelines, p. 5 et seq.; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 70.

1091 Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 5 para. 10.

1092 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 73.

1093 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 73.

1094 Schild, H., GDPR Art. 4', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 18.; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 73.

1095 ECJ, judgement of. 19 October 2016 - C-582/14, ECLI:EU:C:2016:779, para. 46 - Breyer; Kühling, J./Buchner, B./Klar M., GDPR, Art. 4 para. 22.

1096 Simitis, S./Hornung, G./Spiecker, I./Karg, GDPR, Art. 4 No. 1 (59) with further references.

1097 Brink/Eckhardt, ZD 2015, 205, 206 with further references; Kühling, J./Buchner, B./Klar M., GDPR, Art. 4 para. 25.

1098 ECJ, judgement of. 19 October 2016 - C-582/14, ECLI:EU:C:2016:779, p. 45 et seq. - Breyer; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 73; detailed discussion of the entire problem in Kühling, J./Buchner, B./Klar M., GDPR, Art. 4 para. 25 et seq. and in Sydow, G./Marsch, N./Ziebarth, W., GDPR, Art. 4 para. 33 et seq.

However, the anonymisation of personal data alone is not sufficient as a protective measure, as according to Art. 1(2) DGA, the provisions of European data protection law remain unaffected by the provisions of the DGA with regard to personal data. In fact, the relevant European data protection regulations (namely the GDPR) even take precedence over the provisions of the DGA in the event of a conflict pursuant to Art. 1(3) DGA. The consequence is that, according to the literature, access to personal data should only be permitted if the anonymisation is accompanied by a data protection impact assessment pursuant to Art. 35 GDPR, information for data subjects pursuant to Art. 13(1)–(4) and Art. 14(1)–(5) GDPR and the other standard protection mechanisms of the GDPR, in particular if the re-user can only achieve its intended purpose with personal data.[1099] This understanding is probably also based on the EU Commission, according to which re-users may only transfer personal data to third countries in accordance with Chapter V of the GDPR.[1100]

In this respect, it is important to note in practice that the one-dimensional application of these DGA provisions is by no means sufficient. Rather, a compliant application of the law must extend beyond the DGA and incorporate existing European data protection law.[1101]

At this point, the DGA ensures a high level of compliance pressure: as the anonymisation of data by the public body is also a form of processing, this requires an authorisation under the GDPR.[1102] Art. 5 DGA itself is not an authorisation, as the DGA takes a back seat to the GDPR if its scope is open (Art. 1(3) DGA).[1103] Possible authorisations that may come into consideration are, for example, Art. 6 (1)(e) GDPR, Art. 6(1)(c) GDPR or the consent of the data subject pursuant to Art. 6(1)(a) GDPR.[1104]

Contrary to the Commission's original draft, however, there is no hard obligation on public sector bodies to provide support in the event that re-use cannot be authorised and there is no legal basis for the (further) processing of personal data; instead, according to **Art. 5 (6) DGA**, the public sector body must only use its best efforts to assist in obtaining the relevant consent from the data subjects. Presumably, this amendment was intended to protect public sector bodies from being overburdened.[1105]

In addition to the pressure to comply with the GDPR provisions already mentioned, the re-use of publicly collected data for the economic interests of companies is also likely to regularly constitute a change of purpose in accordance with Art. 6(4) GDPR, which is why a case-by-case examination of the compatibility of purposes is required.[1106] This also shows that the DGA teleologically pursues the promotion

[1099] Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 81, 75.
[1100] European Commission, Implementation of the DGA - Guidelines, p. 6.
[1101] Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 75.
[1102] Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 5 para. 13; Roßnagel, A., *ZD* 2021, 188 (189).
[1103] Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 5 para. 13.
[1104] Paschke, A./Rücker, D./Weiden, H., DGA, 1st ed. 2024, Art. 5 para. 15; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 76.
[1105] Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 77.
[1106] Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 79.

of the transfer and accessibility of data, but at the same time is over-organised by the protection dimension of the GDPR because the two regimes are not sufficiently coordinated.[1107]

bb) Protective measures for non-personal data

Data may also be amended or summarised in aggregated form if it concerns business secrets or content protected by intellectual property rights, Art. 5(3)(a) No. ii DGA. If the data is not personal data because personal data has previously been aggregated or processed, no re-identification of data subjects may take place even after disclosure.[1108] If unauthorised further use of data does occur, further users must report this, Art. 5(5) DGA.

In addition to the protection of personal and non-personal data, Art. 5 DGA also regulates the protection of intellectual property and the protection of confidentiality interests. Public bodies can agree **confidentiality obligations** in accordance with Art. 5(5) DGA.[1109] Art. 5(7) and(8) of the DGA oblige data holders to protect intellectual property (7) and to maintain the confidentiality of commercial or statistical confidentiality interests (8) in the event of re-use. For this reason, the **transmission of** data to a re-user located in a **third country** can only take place in accordance with **Art. 5(10) DGA** if the Commission has deemed the regulations of the recipient country for the protection of intellectual property and trade secrets to be equivalent by legal act or if the re-user contractually undertakes to fulfil the conditions of the DGA.[1110] In addition, the Commission is also authorised to lay down further conditions that should apply to the transmission of highly sensitive, non-personal data.[1111]

In addition, according to Art. 5(3)(b), (c) DGA, access to and re-use of data must take place in a secure processing environment provided by the public sector body. According to Art. 2 No. 20 DGA, a secure processing environment is a physical or virtual environment in which all data processing operations can be tracked or supervised. The technical integrity is verified by the public sector body (both remotely and, if necessary, on site).[1112]

Overall, in the case of authorised re-use, public sector bodies are required to impose conditions to ensure the integrity of the operation of the technical systems of the secure processing environment used, Art. 5(4) DGA. This means that the public sector body must create conditions that ensure the integrity and function of the technical systems; the exact conditions are determined by the respective public sector

---

1107 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 79.
1108 Rec. 15 Regulation (EU) 2022/868; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 72.
1109 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 83.
1110 With regard to the contractual obligation, the EU Commission has the option of proposing model contract clauses, European Commission, Implementation of the DGA - Guidelines, p. 6; Tolks, D., *MMR* 2022, 444, (445).
1111 European Commission, Implementation of the DGA - Guidelines, p. 7.
1112 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 82; Tolks, D., *MMR* 2022, 444, (445).

bodies themselves.[1113] With this in mind, it is advisable to introduce cross-agency security standards and certificates within the framework of Art. 5(4) DGA.[1114]

h) Fees for re-use, Art. 6 DGA

Art. 6(1) DGA authorises public sector bodies to levy fees for the authorisation of re-use, provided that they are transparent, non-discriminatory, proportionate and objectively justified and do not restrict competition in accordance with Art. 6(2) DGA.

SMEs, start-ups and other organisations of public interest can justify a reduced fee or even a waiver by justifying a general interest, Art. 6(4) DGA.[1115] This makes it clear once again that the DGA is intended by the European legislator to "proactively" promote data sharing by smaller players in particular[1116], Art. 6(4) DGA.

According to Art. 6(5) DGA, the amount of the fees is determined by the costs associated with the implementation of the application procedure for the re-utilisation of data and depends primarily on the services used; they must be proportionate to the costs and must not restrict competition[1117] . The standard stipulates as a maximum limit that the fees may not exceed the actual costs of the measures associated with the provision.[1118] The specific criteria and methodology for calculating charges are determined internally by the Member States and must be published.[1119]

In addition, Article 6(3) of the DGA requires public sector bodies to also enable the payment of fees online via a cross-border payment service, without discrimination on the basis of the place of establishment of the payment provider, the place of issue of the payment instrument or the location of the payment account in the Union.

Overall, the DGA's requirements for charging fees should be interpreted as an (economic) incentive for the actors involved to reuse data.[1120]

i) Management of re-utilisation procedures, Art. 7, 8, 9 DGA

The provisions on **the management of re-use procedures** aim to support the re-use procedures in technical, organisational and legal terms by obliging the Member States to create competent bodies that act as a central information point (Art. 8(1) DGA) and assist the parties involved in the technical implementation of data re-use (Art. 7(4) DGA). The Member States must provide these competent bodies with the technical and organisational means and the corresponding financial resources to enable them to perform

---

1113 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 4 para. 62.
1114 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 4 para. 62.
1115 Rec. 25 Regulation (EU) 2022/868; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 85.
1116 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 85.
1117 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 85.
1118 Schreiber, K./Schoel, P., *LTZ* 2024, 3 (6).
1119 European Commission, Implementation of the DGA - Guidelines, p. 7.
1120 Schreiber, K./Schoel, P., *LTZ* 2024, 3 (6).

their tasks, Art. 7(3) DGA. Art. 7(4)(a)–(e) DGA lists examples of the individual activities in which the competent authorities are to provide assistance: These include, in particular, advice and technical support in structuring and storing the data in order to make it easily accessible, as well as support in pseudonymising the relevant data sets.

According to Art. 8(1) DGA, the Member States are obliged to establish a "single information point" which receives requests for the re-use of data and forwards them to the competent public sector body.[1121] The task of these central information points is to provide a "single point of contact"[1122] for all interested parties. The information centres should provide information and an overview of where which type of data can be found. For this purpose, the central information centre should maintain a list in accordance with Art. 8(2)DGA, which includes the scope, format and conditions for possible re-use. The list is to be kept electronically and should be accessible to data economy stakeholders. Here too, SMEs and start-ups may be favoured and promoted: There may be a simplified and more efficient application procedure for them in accordance with the provisions of Art. 8(3) DGA.

According to Art. 9 DGA, applications for further processing of data must be processed within two months of the application being submitted, although there may be exceptional extensions of 30 days if the applications are exceptionally extensive and complex. In such cases, the competent public sector body or the authorities referred to in Art. 7 DGA must inform the applicant that more time is needed to complete the procedure, stating the reasons for such a delay.[1123] Irrespective of this, the Member States may, however, set a shorter deadline than the two-month deadline stipulated by the DGA in accordance with Art. 9(1) DGA.[1124] In order to comply with the two-month deadline for processing applications, public bodies should establish standardised procedures for processing applications and prepare their database in such a way that possible access claims can be granted in due time and form.[1125]

j) Criticism

The public sector bodies are left to square the circle[1126] by having to guarantee the protective nature of the data on the one hand and enable its reuse on the other.[1127] In view of the personnel, financial and technical effort involved in implementing the requirements for the provision of data for reuse, it is therefore doubtful whether the economic and social potential of this data will be utilised to a greater extent.

The fact that public bodies are explicitly not obliged to share their data under Art. 1(2) DGA was met with significant controversy, which significantly limits the effectiveness of the DGA with regard to the

1121 Tolks, D., *MMR* 2022, 444 (445).
1122 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 94.
1123 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 9 para. 15 et seq.
1124 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 9 para. 8.
1125 The Bavarian State Commissioner for Data Protection, Data Governance Act Towards a European Single Market for Data - Guidance, para. 56, https://www.datenschutz-bayern.de/infothek/OH_DGA.pdf (last accessed on: 1 November 2024).
1126 Tolks, D., *MMR* 2022, 444 (445).
1127 Tolks, D., *MMR* 2022, 444 (445).

declared goal of increased data use and data sharing.[1128] In addition, important issues such as technical support will continue to depend on national regulations, which contradicts the overarching ideal of harmonised regulation of the data economy across the EU. In particular, companies that operate transnationally within the EU and wish to benefit from the accessibility concept of the DGA may have to comply with several national and more detailed provisions, even though these would have to fulfil certain legally certain requirements in accordance with Art. 4, 5, 6 DGA.

3. Data intermediaries and data intermediation services

The third chapter of the DGA (Art. 10–15 DGA) deals with so-called **data intermediary services**, which are to play a central role in making previously unused data accessible.[1129] Data intermediary services are intended to act as intermediaries by bringing together the supply of data owners and data subjects with the demand of data users.[1130] However, the creation of the legal figure of data intermediary services does not enforce a market; rather, data intermediary services take on the role of a trust-building and mediating intermediary, which is intended to dispel the concerns of data owners and data users and at the same time create incentives for private actors to participate in the development of the data economy.[1131]

a) The term "data intermediation service", Art. 2 No. 11 DGA

Art. 10–15 DGA sets out the obligations for data intermediary services, including the impending consequences in the event of breaches of obligations. According to Art. 2 No. 11, 1st half of the DGA, a **data intermediation service** is a service that is intended to establish business relationships between an indefinite number of data subjects or data owners on the one hand and data users on the other by technical, legal or other means in order to enable the joint use of data, including for the purpose of exercising the rights of data subjects with regard to personal data. According to Art. 2 No. 11, 2nd half of the DGA, the following services may not be provided as negative criteria:

- services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users (a);
- services that focus on the intermediation of copyright-protected content (b);

1128 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 2 para. 2.
1129 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 11, 13; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 2.
1130 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 39, 48; Richter, H., *ZEuP* 2021, 634 (640).
1131 Paschke, A./Rücker, D./Schumacher, P.,/Lücke, M., DGA, 1st ed. 2024, Art. 5 para. 10 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 3.

- services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things (c); and
- data sharing services offered by public sector bodies that do not aim to establish commercial relationships (d).

aa) Initiation of business relationships

One of the key characteristics for the existence of a data intermediation service is the **initiation of a business relationship** in a three-person relationship.[1132] The business relationship then arises between the data holder pursuant to Art. 2 No. 8 DGA or a data subject pursuant to Art. 2 No. 7 DGA on the one hand and a data user pursuant to Art. 2 No. 9 DGA on the other.[1133]



Source: Own illustration

According to Art. 2 No. 9 DGA, a data user is any natural or legal person who has lawful access to data and is authorised to use it for commercial or non-commercial purposes. Even if one could conclude from the German wording of Art. 2 No. 9 DGA that the authorisation to use the data must only exist in the case of personal data, this is a translation error. The use of non-personal data requires authorisation to use the data.[1134] Since the wording only refers to legal persons in general, legal persons under public law and thus public bodies within the meaning of Art. 2 No. 17 DGA are also covered as data users.[1135] Although, according to the wording, they may in principle fall under the definition in Art. 2 No. 9 DGA, data intermediary services are not data users for systematic reasons alone, as Art. 12(a) DGA suggests.

1132 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 65; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 9; Hennemann, M./von Ditfurth, L., *NJW* 2022, 1905 (1908).

1133 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 65; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 9.

1134 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 52, 58; Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 41 et seq.

1135 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 54; in detail Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 37 et seq.; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, §3 para. 12.

Accordingly, the use of the data for which the data intermediary services are provided for own purposes is prohibited, which is why no authorised use of the data is possible.[1136]

The data holder, on the other hand, is the natural or legal person who may grant access to the data and is authorised to disclose it in accordance with Art. 2 No. 8 DGA. However, in the case of a natural person's own personal data[1137], this opens up the subject area of Art. 2 No. 7 DGA (data subject), which corresponds to that of Art. 4 No. 1, first half of the GDPR, so that the term data subject refers to any natural person who is identified or identifiable.[1138]

bb) Practices that constitute data intermediation services

The DGA does not specify how exactly a provider of data intermediation services must provide a service in accordance with Art. 2 No. 11 DGA.[1139] According to recital 28 of the DGA, the European legislator envisaged **data marketplaces** on which companies offer their data as a possible example of a data intermediation service.[1140] It is obvious that operating data marketplaces also means setting up and providing a coherent and appropriate (digital) infrastructure. Other examples that the legislator has in mind as data intermediation services are common European data spaces in which the participants accept certain rules for participation in the ecosystem; data pools set up by companies or natural persons; data cooperatives or unions that have a mechanism for collective consultation or decision-making on the use of data held by the members of the cooperative or union; and finally, personal data wallets or clouds, i.e. services offered to individuals for the storage of personal data currently held by other companies in order to enable the processing of such data by third parties, either within the personal data cloud (the processing algorithm is brought to the data in order to maximise data protection) or by transmissionring such data to third parties.[1141]

Looking at the wording of Art. 2 No. 11 alone, the "match-making"[1142] between data owners and data users is already sufficient to provide a data intermediary service. However, according to the legislator's intention, the mere provision of cloud storage, analytics services, data sharing software, internet browsers or browser plug-ins or email services should not be considered a data intermediary service within the meaning of this Regulation, provided that these services only provide data subjects or data holders

---

1136 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 39; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 55.

1137 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 31; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 50.

1138 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 30; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 49; summarising Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 10.

1139 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 13; similarly Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908)

1140 See Rec. 28 p.4 of Regulation (EU) 2022/868 for further examples of data intermediation services.

1141 European Commission, Implementation of the DGA - Guidelines, p. 9 et seq.

1142 Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908).

with technical tools for sharing data with others, the provision of these tools is neither intended to establish a commercial relationship between data holders and data users nor to enable the provider of data intermediary services to obtain information on the establishment of commercial relationships for the purpose of data sharing.[1143]

Furthermore, it is only those behaviours that can constitute a data intermediation service where the business relationship established **is aimed** precisely at the **joint use of data**. However, this does not mean that several actors use the data simultaneously. Instead, as the definition in Art. 2 No. 10 DGA shows, it refers to the provision of data by a data subject or a data owner to a data user for the joint or individual use of this data, whether in return for payment or free of charge. According to Art. 2 No. 11 DGA, a data intermediary service should therefore provide and therefore share data. This interpretation is supported by a comparison with the other language versions, where, for example, the English language explicitly refers to 'data sharing'.[1144]

Furthermore, only services that are available to an **indeterminate number of data holders and data users** are data intermediation services. The consequence of the fact that the intermediary service must be open to an indefinite number of data holders and data users is that closed data platforms, in which only a pre-defined group of companies may participate, are excluded from the scope (also expressly excluded by Art. 2 No. 11(c) DGA).[1145] However, the requirement of openness leads to problems if the data intermediation service operates in sector-specific data spaces in which only a few players participate in the sharing of data.[1146] In such cases, it depends on whether the data intermediary uses factual, abstract requirements to ensure that actors – provided they fulfil the requirements – can participate in access.[1147] However, if access is subjective or even restricted from the outset, the DGA does not apply to the service.

Finally, as follows from Art. 2(11)(a) of the DGA and recital 28 of the DGA, only those practices are covered with which the data intermediary pursues the intention of establishing a business relationship between the data holder and the data user.[1148] This means that only services aimed at establishing business relationships for the joint use of data are covered.[1149] It is necessary to restrict the definition of a data intermediary service in this way by adding a subjective element, as otherwise there would be a risk

---

1143 Rec. 28 Regulation (EU) 2022/868.

1144 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 15 et seq.

1145 This is also expressly excluded by Art. 2 No. 11(c) DGA; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908); Richter, H., *ZEuP* 2021, 634 (650 et seq.).

1146 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 23.

1147 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 57; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 73; vonDitfurth/Lienemann, CRNI 2022, 270, 280; Richter, H., *ZEuP* 2021, 634 (650).

1148 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 66; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 18.

1149 Schild, H./Richter, H./Schmidt-Wudy, F., 'DGA Art. 2', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 97; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 67.

of proliferation and almost all existing platforms from the B2B sector would be covered by the scope of the DGA.[1150]

cc) No data intermediation services

On the other hand, there is more clarity with regard to behaviour that does not lead to the trader being considered a data intermediary service. On the one hand, recital 28 DGA lists examples of business practices that do not constitute a data intermediary service: According to this, the mere provision of cloud storage, analytics services, data sharing software, internet browsers or browser plug-ins or email services is not a data intermediary service, provided that these services **exclusively** provide data subjects or data holders with **technical tools** to share data with others, the provision of these tools is not aimed at establishing a commercial relationship between data holders and data users, nor does it enable the provider of data intermediary services to obtain information on the establishment of commercial relationships for the purpose of data sharing. On the other hand, Art. 2 No. 11 (a)–(d) DGA also excludes certain types of behaviour by means of a negative list, the existence of which no longer constitutes a data intermediation service within the meaning of the definition.

As already shown (see above), it follows from Art. 2 No. 11(a) DGA that the data intermediary must pursue the intention of establishing a business relationship between the data owner and the data user.[1151] The consequence of this is that so-called 'data brokers', who merely purchase data from a large number of companies in order to process it and then sell it on to other companies, are not covered and are therefore not also data intermediary services.[1152] Similarly, data altruistic organisations are not considered to be data intermediation services on the basis of Art. 2 No. 11(a) DGA, provided that no business relationship is established between the potential data users and data subjects or data holders.[1153] However, if, in exceptional cases, a business relationship is established by a data altruistic organisation, these organisations are nevertheless excluded from the scope of Chapter 3 on the basis of Art. 15 DGA, so that the requirements for data intermediation services do not apply to them. In order to take account of the fact that Art. 2 No. 11(a) DGA is intended to limit the persons covered by the definition, it is also necessary to require that the main purpose of the initiated business relationship is the provision and use of data.[1154]

Pursuant to Art. 2 No. 11(b) DGA, services focussing on the intermediation of copyright-protected content do not constitute a data intermediation service. According to recital 29 DGA, the focus is on the

---

1150 Schild, H./Richter, H./Schmidt-Wudy, F., 'DGA Art. 2', in: BeckOK Datenschutzrecht (49th ed. 2024) para.97); Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 21.

1151 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 66; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 18.

1152 Schild, H./Richter, H./Schmidt-Wudy, F., 'DGA Art. 2', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 98; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908).

1153 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 54; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 6).

1154 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 69; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 21; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908).

intermediation of copyright-protected content if the service is specifically aimed at the intermediation of such content.[1155] However, the intermediation of copyright-protected content does not have to be the sole purpose of the service. Instead, it is sufficient that the communication of copyright-protected content clearly outweighs other purposes.[1156]

The consequence of the exclusion of Art. 2 No. 11(c) DGA is that only those services that are open to an **indefinite number of data holders and data users** are to be regarded as data intermediation services.[1157] Article 2(11)(c) DGA therefore excludes intermediation services that are used exclusively by a data holder to enable the use of data held by that data holder or that are used by several legal entities in a closed group, including supplier or customer relationships or contractual co-operation, in particular where their main objective is to ensure the functionality of objects and devices in the context of the Internet of Things.[1158] The required openness is also given if the use of the service is made dependent on abstract, objective criteria that can be fulfilled by an indefinite number of potential data holders.[1159] If these criteria are established by the data intermediary, the obligation under Art. 12(f) DGA, according to which access must be fair, transparent and non-discriminatory, must be observed in particular.[1160]

Finally, according to Art. 2 No. 11(d) DGA, services offered by public sector bodies without the intention of establishing business relationships are not data intermediary services. Conversely, it follows that services provided by public sector bodies are only data intermediary services if they are offered precisely with the intention of establishing business relationships. The difference to Art. 2 No. 11(a) DGA is that it is based on the de facto establishment of a business relationship.[1161] Despite the fact that the wording of Art. 2 No. 11(d) DGA clearly states that data intermediation services which do not establish a business relationship are excluded, this is a drafting error. (d) should not be understood to mean that services provided by public bodies can also be a data intermediation service without the aim of establishing a business relationship. Even in the case of services provided by public bodies, the decisive factor is whether they are aimed at establishing business relationships through the shared use of data.[1162] The purpose of (d) is to clarify the relationship between the different instruments of the DGA. If public sector

---

1155 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 55.

1156 Schild, H./Richter, H./Schmidt-Wudy, F., 'DGA Art. 2', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 99.

1157 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 57; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 73.

1158 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 57; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 73.

1159 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 73; von Ditfurth, L./Lienemann, G., *CRNI* 2022, 270 (280); Richter, H., *ZEuP* 2021, 634 (650 et seq.).

1160 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 57; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 73.

1161 Paschke, A./Rücker, D./Keppeler, L./Poncza, M., DGA, 1st ed. 2024, Art. 2 para. 60.

1162 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 75; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 19 et seq.

bodies merely enable the re-use of data from their de facto technical control, but do not aim to establish a business relationship, they are not data intermediary services.[1163]

dd) Summary

Overall, it can be stated that the definition of data intermediation service according to Art. 2 No. 11 DGA is a two-part definition, in that the first half of the definition positively determines which properties characterise data intermediation service and this is then supplemented and concretised by the negative list of the second half.[1164] A data intermediation service therefore only exists if an indefinite number of business relationships can be initiated with the aim of sharing data. On the other hand, it is not a data intermediation service if the aim is not to establish a business relationship between data owner and data user, where the focus is on the brokerage of copyright-protected content, if the service is not open to an indefinite number of data holders and data users or if a public body offers data brokerage to bodies without the intention of establishing business relationships.

b) Obligations of data intermediation services

If a data intermediation service is provided, the requirements of the third chapter (Art. 10–15 DGA) apply to it. In this context, the provider of the data intermediation service is obliged to register in accordance with Art. 11 DGA as well as a comprehensive catalogue of obligations in accordance with Art. 12 DGA, which must be fulfilled when providing the service. However, the obligation to register and the catalogue of obligations only apply if it is a data intermediation service within the meaning of Art. 10 DGA.

aa) Data intermediation service within the meaning of Art. 10 DGA

The mere fact that a data intermediation service within the meaning of Art. 2 No. 11 DGA exists does not mean that the provider is also subject to special obligations. Instead, Art. 10 DGA further restricts the scope by declaring Art. 11 et seq. applicable to only three types of data intermediation services.[1165]

(1) Intermediary services between data holders and potential data users, Art. 10(a) DGA

According to Art. 10(a) DGA, data brokering services between data holders and potential data users, including the provision of technical and other means as a prerequisite for such services, are subject to the further provisions of Art. 11 et seq. DGA. The services covered may also include those that enable

---

1163 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 75; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 33.

1164 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 2 para. 64; Schild, H./Richter, H./Schmidt-Wudy, F., 'DGA Art. 2', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 90.

1165 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 10 para. 6; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 10 para. 1.

the bilateral or multilateral exchange of data or the establishment of platforms or databases that enable the exchange or sharing of data, as well as the establishment of other specialised infrastructures for the interconnection of data holders with data users.[1166] Since (a) explicitly only refers to data holders and data users, it does not cover intermediary services where the data intermediary mediates data between data subjects (Art. 2 No. 7 DGA) and data users. Instead, in such cases, this is an intermediary service covered by Art. 10(b) DGA.[1167] The consequence of the fact that the wording refers to potential data users is that **no actual use** of the data is required in order for a data intermediary to fulfil the obligations under Art. 11 et seq. DGA is present. The addition, including the provision of technical or other means, extends the scope of Art. 10 DGA to services that carry out ramp activities, provided that their objective is data brokering.[1168] The intermediary services mentioned in Art. 10(a), 2nd half of the DGA are a non-exhaustive list of intermediary services that fall within the scope of Art. 10(a) DGA.[1169]

(2) Intermediary services between data subjects or natural persons and data users, Art. 10(b) DGA

The second category of intermediary services to which Art. 11 et seq. DGA apply are, according to Art. 10(b) DGA, intermediary services between data subjects who wish to make their personal data accessible or natural persons who wish to make non-personal data accessible and potential data users. The DGA does not provide a definition for the term "**making available"**. However, it can be inferred from the general use of the term and the use of the term in other parts of the DGA that it refers to the **granting of access** to data.[1170] Since it only covers the case that data subjects make their personal data accessible, intermediary services between data subjects who either want to make personal data that only concerns third parties accessible or do not want to make any data accessible at all do not constitute intermediary services within the meaning of Art. 10(b) DGA.[1171]

(3) Services of data cooperatives, Art. 10(c) DGA

Finally, Art. 10(c) DGA extends the scope of Art. 11 et seq. DGA **to the services of data cooperatives**. The term "data cooperative" is defined in Art. 2 No. 15 DGA as data intermediation services offered by an organisational structure composed of data subjects, one-person companies or SMEs that are members of this structure, and whose main purpose is to assist its members in exercising their rights in relation to certain data, including in making an informed decision before consenting to data processing, exchanging

---

1166 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 10 para. 9; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 10 para. 17.

1167 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 10 para. 19.

1168 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 10 para. 23; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 10 para. 22.

1169 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 10 para. 26.

1170 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. para. 35; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 10 para. 35.

1171 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 10 para. 36.

views on the purposes and conditions of data processing best suited to the interests of their members in relation to their data, and negotiating the conditions of data processing on behalf of members prior to granting permission to process non-personal data or consenting to the processing of personal data. Like data intermediation services under Art. 10(b) DGA, the services of data cooperatives relate to both personal and non-personal data. However, Art. 10(c) DGA goes beyond (b) in that the services of data cooperatives can also be offered to one-person companies or SMEs and the data cooperative can provide support even before consent is given.[1172]

bb) Registration according to Art. 11 DGA

Before the provider of data brokering services can provide its services, it must register with the competent authority, Art. 11(1) DGA. According to recital 38, the aim of the registration procedure is to create a trustworthy environment on the basis of which data can then be transmitted, shared and used between data holders, data subjects and data users.[1173] Contrary to what was initially considered, the Commission has thus decided against a certification system, as this would have had a deterrent effect, particularly with regard to start-ups.[1174] Instead, the provider is subject to a pure registration obligation (**prohibition with reservation of registration**[1175]). In particular, the provider does not have to wait for authorisation from the competent authority after registration, but can start operating immediately after registration.[1176] It is therefore up to the providers to check independently and at their own risk whether their business model constitutes a data intermediation service in accordance with Art. 10 DGA.[1177]

For Germany, the competent authority for the notification procedure has not yet been finalised. The draft law implementing the DGA provides for the **Federal Network Agency** as the competent authority for the notification procedure in Section 2(1) No. 1 of the Data Governance Act.[1178]

According to Art. 11(2) DGA, the registration must be made in the Member State where the provider has its main establishment. In the case of a provider that is not established in the Union, the provider must appoint a legal representative in accordance with Art. 11(3) DGA, who acts as a point of contact for the competent authorities for questions relating to the data intermediation services provided. However, the appointment of the legal representative does not mean that the legal representative is liable for

---

1172 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 10 para. 56.

1173 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 11 para. 3; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 47.

1174 COM(2020) 767 final, p. 6; Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 11 para. 4; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 49.

1175 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 11 para. 2; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 11 para. 17.

1176 Schröder, M., 'DGA Art. 11' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 19; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 11 para. 23; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 50.

1177 Gellert, R./Graef, I., *TILEC* Discussion Paper 2021-006, 9; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1907).

1178 Draft bill of the Federal Ministry for Economic Affairs and Climate Protection, Draft Act on the Implementation of the EU Regulation on European Data Governance, p. 5.

violations of the DGA, but that the actual provider remains fully responsible.[1179] The background to this regulation is to prevent companies from evading regulation by the DGA by relocating their establishment to a third country.[1180] Instead, the provisions of the DGA also apply to a provider that has its establishment in a third country if it clearly intends to reach persons in one or more Member States with its offer.[1181]

The information that must be included in the notification is standardised in Art. 11(6) DGA. If the information changes after the notification, the provider must notify the competent authority, Art. 11(12) DGA. The provider may request confirmation of the registration from the competent authority in accordance with Art. 11(8) DGA. However, confirmation of registration is not required to commence the activity. According to Art. 11(4) DGA, mere registration is sufficient.[1182] If a provider of data intermediation services ceases its activities, it must notify the competent authority within 15 days in accordance with Art. 11(13) DGA.

The competent authorities of the Member States are obliged under Art. 11(10) and 14 DGA to inform the Commission of every notification, amendment to the notification and deregistration. On the basis of this notification, the Commission creates a **register** listing all data intermediation services that provide their services in the European Union, Art. 11(10) DGA.[1183] As of October 2024, nine companies from Finland, France and Hungary are listed there as data intermediation services.[1184]

cc) Catalogue of obligations under Art. 12 DGA

The core component of the regulations for data brokering services is the catalogue of obligations in Art. 12 DGA. The purpose of the catalogue is to strengthen trust in the use of data intermediation services in order to promote the sharing of data.[1185] At the same time, however, potential competitive risks from data brokerage platforms should be prevented in advance.[1186]

Firstly, Art. 12(a) DGA standardises **the principle of neutrality** of a data intermediation service with regard to the handling of the data provided.[1187] The data intermediation service is obliged to maintain strict neutrality with regard to the data to be exchanged between the data owner and the data user. It may

---

1179 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 55.

1180 Schröder, M., 'DGA Art. 11' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 14; Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 11 para. 56.

1181 Rec. 42 Regulation (EU) 2022/868; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 57.

1182 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 11 para. 14; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 75 et seq.

1183 Schröder, M., 'DGA Art. 11' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 40 et seq; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 80.

1184 https://digital-strategy.ec.europa.eu/de/policies/data-intermediary-services (last accessed on: 1 November 2024).

1185 See also Rec. 32 of Regulation (EU) 2022/868; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 10 para. 20.

1186 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 10 para. 20; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1907).

1187 Similarly Steinrötter, B./Savary, F., Europäische Plattformregulierung, § 19 para. 29; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 32.

not use the data exchanged via its platform for purposes other than making it accessible to the respective data users.[1188] There is therefore a strict separation of data exchange and use. The consequence of this is that, in accordance with Art. 12(c) DGA, the operator of the data brokerage platform can only use the metadata generated during the performance of the brokerage services to improve its own platform.[1189] An exception to the strict purpose limitation is provided for in Art. 12(d) DGA, according to which the conversion of data for specific purposes is permitted.[1190] In addition to this **principle of prohibition of processing**[1191], Art. 12(a) DGA also contains a **prohibition of vertical integration**[1192]. This prohibition of vertical integration ensures that, according to recital 33 DGA, there must be a structural separation of the data intermediation service from all other services provided. The data switching service must therefore be provided by a legal entity that is separate from the provider's other activities.[1193] The exact requirements for this separation are not clear. However, it will probably not be required that the data intermediation service must be independent of any parent company in terms of instructions and economic independence.[1194] Instead, it can be concluded from a reverse conclusion to Art. 12(b) DGA that a structural spin-off into a subsidiary within a group structure is considered sufficient.[1195] If a company wishes to provide data intermediation services in addition to its existing business area, it is therefore advisable to carry out a structural separation and have the brokerage services provided by a separate legal entity so that the neutrality requirement pursuant to Art. 12(a) DGA is preserved in the best possible way.[1196]

Art. 12(b) DGA establishes a **prohibition of tying transactions.** It is important to note that the data intermediary service is not permitted to make its terms of use, including its fees, contingent upon the

---

1188 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 5; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908).

1189 Schröder, M., 'DGA Art. 12' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 25; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908).

1190 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 5; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 34.

1191 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 33.

1192 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 32.

1193 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 9; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 36; von Ditfurth, Datenmärkte, Datenintermediäre und der Data Governance Act, p. 362; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908).

1194 von Ditfurth, Datenmärkte, Datenintermediäre und der Data Governance Act, p. 364; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908) et seq.; Richter, H., *ZEuP* 2021, 634 (654); Spindler, G., *CR* 2021, 98, (104).

1195 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 36; von Ditfurth, Datenmärkte, Datenintermediäre und der DataGovernance Act, p. 362; see also European Commission, Umsetzung des DGA - Leitfaden, p. 12; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 92.

1196 For more details on the prohibition of vertical integration, see Ditfurth, Datenmärkte, Datenintermediäre und der DataGovernance Act, p. 359 et seq.; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1908).

utilisation of other services provided by the intermediary[1197] or its affiliated parent or sister companies[1198] . It is therefore inadmissible for the user of a data intermediation service to receive more favourable conditions solely on the basis of the fact that he uses other services of the data broker, a parent company or a sister company.[1199] The background to this prohibition is to prevent gatekeepers within the meaning of the Digital Markets Act from establishing themselves as data intermediation services and then disrupting competition and data intermediation services.[1200] It is also important to note that the ban on tying does not apply to data subjects who may also be users of a data intermediation service.[1201]

The duty of conduct in Art. 12(c) DGA provides **for a restriction on the use of metadata** collected by the data intermediation service in connection with the provision of the service. This data may only be used for the further development of the data intermediation service, to detect fraud or in the interests of cyber security.[1202]

Furthermore, Art. 12(d) DGA stipulates that the provider of the data intermediary service must enable the exchange of data in the format in which it was transmitted to it. The provider may only convert the data if one of the authorisation conditions listed in (d) applies.[1203] The cases in which data may be converted are Improvement of interoperability within and between sectors through the conversion, data user has requested conversion, Union law requires the conversion or the conversion serves to harmonise with international and European data standards.[1204] The behavioural obligation aims to improve the usability of data[1205] and remove barriers to data sharing.[1206]

Art. 12(e) DGA provides **for a restriction on the tying of services.** Accordingly, providers of data intermediaries may only combine their services with additional offers to a limited extent. Only coupling

---

1197 Rec. 33 Regulation (EU) 2022/868 contains an exemplary overview of possible services that would also have to be utilised.

1198 Schröder, M., 'DGA Art. 12' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 20; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 39, critical of whether sister companies should also be covered.

1199 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 95; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909).

1200 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 10; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 38; Picht/Richter, GRUR Int. 2022, 395, 399; von Ditfurth, L./Lienemann, G., *CRNI* 2022, 270 (284 et seq.).

1201 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 38; Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 11; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 96.

1202 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 13; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 97.

1203 Schröder, M., 'DGA Art. 12' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 33; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 48.

1204 Steinrötter, B./Savary, F., Europäische Plattformregulierung, § 19 para. 32; Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 16.

1205 Schröder, M., 'DGA Art. 12' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 34; Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12, para. 17.

1206 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 48; von Ditfurth, L./Lienemann, G., *CRNI* 2022, 270, (2839); Richter, H., *ZEuP* 2021, 634, (654).

with specific tools (technical means of software and hardware that facilitate data exchange[1207]) and services for data holders or data subjects that facilitate data exchange is permitted.[1208] It could be inferred from the wording ("in particular") that the additional tools and services may also be offered for other purposes in addition to facilitating the exchange of data. However, when comparing the English and French versions of the regulation, it is clear that this is a drafting error. In the other versions, the use of tools and services is only permitted to improve data exchange.[1209] The tools may only be used at the express request or with the consent of the data holder or the data subject. An active approach to the data intermediary is therefore required.[1210] However, there is no consensus on whether implied consent is sufficient. However, the fact that the word "expressly" only refers grammatically to the word "request" speaks in favour of implied consent.[1211] If the data intermediary legitimately uses third-party tools (Art. 12(e) DGA at the end), the strict purpose limitation principle also applies to the use of these tools, which is why the third party may not use the tool for any other purpose than to facilitate the data exchange.[1212] Art. 12(f) DGA imposes a **transparency requirement** and a **prohibition of discrimination** on providers of data intermediation services. The access terms and conditions of data intermediation services must be fair, transparent and non-discriminatory.[1213] The purpose of the ban on discrimination is to prevent distortions of competition and market foreclosure. Small and medium-sized enterprises and start-ups in particular should be able to gain access to data intermediation services under the same conditions.[1214] The transparency requirement, on the other hand, is intended to promote competition by enabling a comparison of offers.[1215] However, the ban on discrimination only prohibits unequal treatment that is not objectively justified, meaning that it must ultimately always be assessed on a case-by-case basis whether there is an objective reason that justifies the unequal treatment.[1216] However, it is unclear which requirements are to be placed on the transparency requirement in detail. Due to the lack of concretisation by the legislator and the fact that transparency obligations are a reaction to a market failure that has not

---

1207 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 21.

1208 Schröder, M., 'DGA Art. 12' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 45; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 100.

1209 Schröder, M., 'DGA Art. 12' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 45; Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 23.

1210 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 24; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 61.

1211 a.A. Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 61, according to which an implied declaration is not sufficient; Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 25.

1212 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 27; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 101.

1213 Steinrötter, B./Savary, F., Europäische Plattformregulierung, § 19 para. 34; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909).

1214 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 31; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 103; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909).

1215 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 32; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909); Richter, H., *ZEuP* 2021, 634 (656).

1216 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 103; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909).

yet been identified in relation to data intermediation services, the transparency requirement can be considered to be fulfilled if the parties are in a position to understand the requirements and the process of data brokerage.[1217] On the other hand, it is also possible that the transparency obligations are only considered to be fulfilled if fees and other conditions are disclosed to potential platform users and a comparison of the offers is therefore possible.[1218]

Finally, Art. 12 (g), (h), (j), (k), (l), (o) DGA standardise a series of **monitoring and security obligations**.[1219] For example, Art. 12(g) DGA obliges providers of data intermediation services to take precautions to prevent fraudulent or abusive practices in relation to the data user.[1220] Art. 12(h) DGA prescribes the taking of precautions in the event of insolvency.[1221] According to Art. 12(j) DGA, the data intermediation service must take appropriate technical, legal and organisational measures to prevent the unlawful transmission of non-personal data.[1222] As the data intermediation service is only obliged to take appropriate measures, it is not obliged to ensure the legally compliant behaviour of users.[1223] According to Art. 12(k) DGA, the data holder must be informed of any unauthorised access to data and Art. 12(l) DGA standardises the obligation to maintain an appropriate level of security when storing, processing and transmissionring non-personal data.[1224] Art. 12(o) DGA establishes an obligation to keep a record of data processing activities.[1225]

c) Law enforcement

The Member States are responsible for monitoring and implementing the DGA.[1226] They must designate a competent authority to enforce the law, whereby, according to Art. 26(2) DGA**, no new authority** has to be created, but one or more existing authorities can be entrusted with the enforcement of the law. In the case of an inter-European matter, the competent authorities of the Member States must exchange information and co-operate in accordance with Art. 14(7) DGA. According to the Federal Ministry for

---

1217 So only Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 67.

1218 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 103; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909); Richter, H., *ZEuP* 2021, 634 (656).

1219 Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909).

1220 Steinrötter, B./Savary, F., Europäische Plattformregulierung, § 19 para. 35; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 68.

1221 In detail Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 12 para. 70; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910).

1222 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 41; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909).

1223 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 12 para. 44; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 111; a.A. Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909), according to which the data brokerage service has an obligation to monitor the data transactions of its users and to prevent legal violations itself.

1224 Steinrötter, B./Savary, F., Europäische Plattformregulierung, § 19 para. 39 et seq.; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910).

1225 Steinrötter, B./Savary, F., Europäische Plattformregulierung, § 19 para. 43; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 120.

1226 Steinrötter, B./Savary, F., Europäische Plattformregulierung, § 19 para. 46; Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 122.

Economic Affairs and Climate Protection's draft bill for a law to implement the EU Regulation on European data governance, the competent authority in Germany will be the Federal Network Agency.[1227]
According to Art. 14(1) DGA, the competent authority has a comprehensive **monitoring and supervision obligation** in connection with providers of data intermediation services.[1228] It can either take action itself ex officio or monitoring or supervision can also be carried out at the request of third parties.[1229] As part of its monitoring and supervision obligation under Art. 14(2) DGA, the competent authority is authorised to request information that is necessary to comply with the provisions of Chapter 3 of the DGA. The competent authority therefore has a right to information, meaning that the data intermediary is obliged to provide the information.[1230]
If the authority discovers a breach of Art. 10 et seq. DGA, it must inform the provider of the data intermediation service of the violation in accordance with Art. 14(3), 1st half of the DGA (notification obligation). Following this notification, the provider must be given the opportunity to comment within 30 days in accordance with Art. 14(3) DGA.
If a provider is in breach of Art. 10 et seq. DGA, Art. 14(4) DGA contains a catalogue of measures that the competent authority can take to ensure compliance with the provisions of the DGA. According to Art. 34(1) DGA, it is left to the Member States to standardise further sanctions.[1231] In general, the competent authority is authorised under Art. 14(4) DGA to order the cessation of a specific infringement and, within the framework of a **general clause-like authorisation,** to adopt appropriate and proportionate measures to ensure compliance. In addition, Art. 14(4)(a)–(c) DGA lists specific measures that can be taken by the authority.[1232] The measures include **fines and periodic penalty payments** (a), **postponement of the start** or **suspension of the provision of** the data intermediation service (b) and **cessation** of the provision of the data intermediation service (c). As the most severe measure, the cessation of the provision of the data intermediation service pursuant to (c) is only possible in the event of a serious or repeated infringement which has not been remedied despite prior notification pursuant to Art. 14(3) DGA. The decisive criterion for determining the seriousness of the offence is the risk to the legal interests at stake.[1233] The catalogue of Art. 34(2) DGA can be used as further criteria.[1234] In the context of

---

1227 Section 2 (1) DGG-E, draft bill of the Federal Ministry for Economic Affairs and Climate Protection, Draft Act on the Implementation of the EU Regulation on European Data Governance, p. 5.
1228 Paschke, A./Rücker, D./Wernicke, A., DGA, 1st ed. 2024, Art. 14 para. 8; Richter, H., 'DGA Art. 14' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 5.
1229 Paschke, A./Rücker, D./Wernicke, A., DGA, 1st ed. 2024, Art. 14 para. 8; Richter, H., 'DGA Art. 14' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 7.
1230 Paschke, A./Rücker, D./Wernicke, A., DGA, 1st ed. 2024, Art. 14 para. 16; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 14 para. 24.
1231 Paschke, A./Rücker, D./Wernicke, A., DGA, 1st ed. 2024, Art. 14 para. 23 et seq.
1232 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 14 para. 32.
1233 Paschke, A./Rücker, D./Wernicke, A., DGA, 1st ed. 2024, Art. 14 para. 36; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 14 para. 58.
1234 Paschke, A./Rücker, D./Wernicke, A., DGA, 1st ed. 2024, Art. 14 para. 36 et seq.; for a detailed description of the factors under consideration, see Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 14 para. 58.

repeated offences, it follows from the meaning and purpose of compliance with the provisions of Chapter 3 that only a certain frequency of offences is relevant and not whether an offence has been committed repeatedly or whether several offences have been committed.[1235] The mere existence of a risk of repetition is not sufficient.[1236]

d) Criticism

However, the regulations of the DGA with regard to data intermediation services are not all positive. Instead, there are also a number of points that need to be criticised.

Right from the start, the definition of the term "data intermediary service" under Art. 2 No. 11 DGA is **too vague**. According to this, the sharing of data does not have to be the main purpose of the initiated business relationship. However, since data is shared in almost every business relationship nowadays, there is a risk that a data intermediation service pursuant to Art. 2 No. 11 DGA is almost always present.[1237]

Furthermore, the regulation on notification under Art. 11 DGA and the supervisory framework of the competent authority under Art. 14 DGA must also be critically scrutinised. Compared to the existing legal provisions in the area of data protection and IT security law, the provisions of the DGA are stricter and their usefulness is also questionable, as the sharing of data is more likely to fail due to technical problems than due to a lack of legal regulation.[1238] On the other hand, it is certain that the DGA regulations will increase the compliance costs of companies wishing to offer a data intermediation service and limit the scope for new business models in the area of data sharing.[1239] A possible alternative proposal, which would significantly reduce the regulatory density in the area of the notification and supervisory framework, would have been the **introduction of a voluntary certification system** instead of the prohibition with notification requirement[1240].[1241] As there is only an 'ex-post control' by the authorities despite the prohibition with reservation of notification[1242] , it must also be questioned whether the lack of trust can be created in this way so that data intermediation services are used.[1243]

1235 Paschke, A./Rücker, D./Wernicke, A., DGA, 1st ed. 2024, Art. 14 para. 38; probably also Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 14 para. 57.

1236 Paschke, A./Rücker, D./Wernicke, A., DGA, 1st ed. 2024, Art. 14 para. 38.

1237 Generally critical of the definition Schild, H./Richter, H./Schmidt-Wudy, F., 'DGA Art. 2', in: BeckOK Datenschutzrecht (49th ed. 2024) para. 90; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909).

1238 Specht-Riemenschneider, L./Blankertz, A., *MMR* 2021, 369, (370); Spindler, G., *CR* 2021, 98, (104); Tolks, D., *MMR* 2022, 444, (447).

1239 Particularly critical of the higher costs are Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 10 para. 68, Art. 11 para. 88; Tolks, D., *MMR* 2022, 444, (447).

1240 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 11 para. 2; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 11 para. 17.

1241 Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910); Tolks, D., *MMR* 2022, 444, (447); Hartl, K./Ludin, J., *MMR* 2021, 534, (537); Specht-Riemenschneider, L./Blankertz, A., *MMR* 2021, 369, (370) in detail on the idea of the certification system.

1242 Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 11 para. 2; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 11 para. 17.

1243 Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910).

In principle, the purpose pursued by the prohibition of tying (Art. 12(b) DGA) in the form of preventing the anti-competitive effects of such transactions is to be assessed positively.[1244] However, such tying transactions can also have favourable effects on competition.[1245] The general prohibition under Art. 12(b) DGA, which does not provide for an exception, is therefore not to be welcomed without reservation. Another criticism of the catalogue of obligations in Art. 12 DGA is that it sometimes leads to **considerable legal uncertainty** for data intermediaries.[1246] With regard to the interoperability obligation under Art. 12(i) DGA, there is currently a lack of standards for data intermediation services, which is why it is unclear what measures must be taken by data intermediaries. Only in the long term will common standards be developed by the European Data Innovation Board.[1247] Furthermore, the DGA abstains on the question of what constitutes an appropriate measure within the meaning of Art. 12(j) DGA[1248], with the result that the legal uncertainty for data intermediaries is further increased.

Finally, a general criticism of the legal provisions for data intermediation services is that they represent a departure from the previous principles of antitrust law. Whereas previously there was an ex post behavioural test based on general and flexibly formulated standards, the DGA leads to the **imposition of 'ex ante' behavioural obligations** with regard to data intermediation services. The consequence is that it is not possible to take pro-competitive effects into account and data intermediation services are regulated regardless of their market power.[1249] This makes it very difficult for providers of data intermediation services to achieve a dominant market position. At the same time, there is a real risk that these strict requirements will inhibit innovation by data intermediaries in the long term.[1250] Ultimately, this puts data intermediation services at a disadvantage compared to similar business models, such as 'data brokers' or closed data platforms, which are not covered by the definition of a data intermediation service, which is why **evasive action** is to be expected.[1251] Overall, there is therefore a lack of incentives for companies to operate as data intermediation services on the data market.[1252]

1244 von Ditfurth, M., Data Markets, Data Intermediaries and the Data Governance Act, p. 376.

1245 Similarly Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 117; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909); on the positive effects on competition Schweitzer, H., *ZEuP* 2021, 503, (537).

1246 In this sense, Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 10 para. 69.

1247 Schreiber, K./Pommerening, P./Schoel, P., DGA, 2023, § 3 para. 109; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1909).

1248 Schröder, M., 'DGA Art. 12' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 68; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910).

1249 Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910).

1250 Similarly Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 117; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910).

1251 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 117; Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910); in more detail on possible evasive movements Richter, H., *ZEuP* 2021, 634 (662 et seq.).

1252 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 117; Paschke, A./Rücker, D./Schumacher, P./Lück, M., DGA, 1st ed. 2024, Art. 10 para. 68.

4. Data altruism, Art. 16–25 DGA

The DGA introduces another institutional novelty in data law with **data altruism**. The regulations for this voluntary, unpaid form of data sharing can be found in the fourth chapter (Art. 16–25 DGA). Art. 16 DGA initially opens up the possibility for Member States to adopt national provisions to facilitate data altruism. Art. 17–19 DGA regulate the registration and listing of data altruism organisations, whose transparency, protection and procedural requirements are set out in Art. 20–22 and Art. 25 DGA. Provisions regarding law enforcement can be found in Art. 23, 24 DGA.

a) Concept, function and principle of data altruism

The term data altruism is defined by Art. 2 No. 16 DGA and makes it clear that data altruism can relate to both personal and non-personal data and also sets out further requirements that must be met in order to be subject to the provisions of the DGA with the criteria of voluntariness, gratuitousness and altruistic pursuit of objectives.[1253]

Data altruism is intended to ensure that more personal and non-personal data is shared in line with the data strategy. Altruism therefore lies in **making** the innovation potential inherent in data **available free of charge**.[1254] Specifically, data altruism means the voluntary "disclosure of data without commercial self-interest"[1255] with the consent of the data subjects, provided the data is personal data, Art. 2 No. 16 DGA. The fact that data altruism is supposed to lack remuneration does not rule out compensating the sharer for the costs incurred as a result of the disclosure. Both data subjects and data holders can be compensated.[1256]

The regulations on data altruism – like the other provisions of the DGA – represent a structural measure: They are intended to reduce currently existing inhibitions regarding data sharing and create an environment in which sharing is encouraged. In this respect, the DGA provides a framework for organisations to voluntarily establish themselves in order to process altruistically provided data. The legal framework is intended to be a breeding ground for data altruistic organisations, which are entered in a register after free foundation and are to manage the data received from "**data donations**".[1257]

In line with the concept of altruism, the regulations on data altruism are not primarily intended for companies operating on the data market. Instead, the regulations are primarily aimed at the general public, although this does not rule out the possibility that companies may still benefit from them.[1258] In this

---

1253 Rachut, S., *ZD* 2024, 248, (249).
1254 SWD (2020) 295 final, p. 1 et seqq.
1255 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 16 para. 9.
1256 Paschke, A./Rücker, D./Heckmann, D., DGA, 1st ed. 2024, Art. 16 para. 98; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 16 para. 11.
1257 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, 2023, § 4 para. 4-6.
1258 von Hagen, P./Völzmann, L., *MMR* 2022, 176, (176); https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained (last accessed on: 1 November 2024).

respect, one could speak of a data donation, as has already been discussed in the literature.[1259] However, terms such as "data provision"[1260] or data disclosure are probably more appropriate than "data donation". The term "**altruistic data disclosure"**[1261] is particularly precise because, despite the ongoing legal procedural sovereignty of the data subject, it implies that an altruistic disclosure is accompanied by a loss of informational exclusivity, which can reduce the monetary value of the data in economic terms.

In the future, European legislators hope that the principle of data altruism will lead to the release of large amounts of data. So much so that the practicability of data analyses will be promoted within Europe, which should also benefit machine learning.[1262] The altruistic disclosure of data should also benefit healthcare, the mobility sector and the fight against climate change. Last but not least, the member states are also likely to have a great interest in data disclosure: The aim is to improve public services, enrich statistics and make government decision-making more efficient.[1263]

b) National arrangements for data altruism, Art. 16 DGA

The principle of data altruism is literally opened up by the DGA in Art. 16. However, Art. 16 DGA is not so much a standard concretising the concept of data altruism as an **opening clause**.[1264] Thus, Art. 16 p. 1, 2 DGA addresses the Member States, which can organise the concrete form of practical data altruism themselves. In this respect, Art. 16 DGA is less of a regulation and more of a directive.[1265] Art. 16 sentence 2 DGA leaves the issue to the Member States as a question of political-strategic organisation.[1266] The Member States can make use of organisational or technical regulations (or both) and define national strategies. According to recital 45 DGA, this refers to measures that would facilitate data altruism. For example, data subjects or data holders could be provided with easy-to-use tools to give consent or authorisation for altruistic use of their data. Strategies under Art. 16 DGA would also include awareness-raising campaigns and improved exchange between national authorities.

c) Recognised data altruism organisations, Art. 17–19 DGA

Pursuant to Art. 17 et seq. DGA, legal entities that strive to promote the objectives set out in the definition of data altruism (Art. 2 No. 16 DGA) may register as **data altruism organisations** recognised in the Union, provided that they do not operate for profit, are legally independent and also comply with

---

1259 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 16 para. 5, critical of the concept of data donation, according to which this concept is misleading, as the provider has no minus on its side; with regard to corona apps Kühling/Schildbach, *NJW* 2020, 1545; specifically on the data altruism of the DGA von Hagen, P./Völzmann, L., *MMR* 2022, 176, (176).

1260 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 5.

1261 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 16 para. 5.

1262 Rec. 45 Regulation (EU) 2022/868.

1263 Rec. 4 Regulation (EU) 2022/868, in detail Paschke, A./Rücker, D./Heckmann, D., DGA, 1st ed. 2024, Art. 16 para. 45-51.

1264 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 16 para. 1.

1265 Paschke, A./Rücker, D./Heckmann, D., DGA, 1st ed. 2024, Art. 16 para. 1.

1266 Paschke, A./Rücker, D./Heckmann, D., DGA, 1st ed. 2024, Art. 16 para. 1; Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 16 para. 34; Rachut, S., *ZD* 2024, 248, (249).

extensive transparency and record-keeping obligations.[1267] A data altruism organisation can also be a data intermediation service under the DGA; there is no exclusive relationship between the two organisations.[1268]

Art. 17(1) DGA initially prescribes registers at national level, which are to be established by the respective competent authority. Data altruism organisations can become a recognised organisation by registering in such a register – however, registration is not mandatory for data altruistic activities.[1269] In addition, the Commission maintains a Europe-wide register of all registered organisations for information purposes in accordance with Art. 17(2) DGA. As of October 2024, only one data altruism organisation operating in Spain had been registered.[1270] In addition to the registers, Art. 17(2) DGA also provides for a common logo for data altruism organisations.[1271] The logo to be designed and introduced by the Commission must be displayed on all publications of the organisations that are related to their altruistic function. The registration and the uniform logo of data altruism organisations recognised in the Union should, according to the hopes of the legislator, contribute to a de facto leap of faith. They also signal the legal difference between data altruism organisations and data intermediation services.[1272] Data intermediation services are exempt from the provisions of the chapter on data intermediation services (Art. 15 DGA).

Art. 18 DGA describes how a data altruism organisation obtains the status of a recognised organisation, i.e. which qualitative requirements an organisation must meet in order to be registered: It lists five requirements for inclusion in the register, which are intended to ensure that only those organisations that clearly comply with the principle of Art. 2 No. 16 DGA are included. These include

- Carrying out data altruistic activities (a);
- own legal personality in accordance with national law (b);
- Non-profit activities and legal independence from an organisation that pursues profit-making objectives (c);
- functional separation of data altruism activities from other activities of the organisation (d);
- Compliance with the requirements of the regulations to be issued by the Commission pursuant to Art. 22(1) DGA (e).

Only these organisations should be entitled to any benefits, such as the use of the joint logo. Art. 19 DGA sets out exactly how registration is formally carried out. According to this, registration takes place

1267 Tolks, D., *MMR* 2022, 444, (447).
1268 Hornung, G./Schomberg, A., *CR* 2022, 508, (512); Rachut, S., *ZD* 2024, 248, (249).
1269 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 17, para. 1.
1270 https://digital-strategy.ec.europa.eu/de/policies/data-altruism-organisations (last accessed on: 1 November 2024).
1271 The logo designed by the Commission can be viewed here: https://digital-strategy.ec.europa.eu/de/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union (last accessed on: 1 November 2024).
1272 Tolks, D., *MMR* 2022, 444, (447).

at the request of an organisation willing to register, Art. 19(1) DGA.[1273] Organisations not established in the Union also require a legal representative, Art. 19(3) DGA.

The legal consequence of registering a data altruism organisation is its official recognition, which is intended to promote trust in legal transactions. In practice, this is expressed through the right or obligation to use the joint logo in accordance with Art. 17(2) DGA.[1274]

d) Transparency, protection and procedural requirements of data altruistic organisations, Art. 20–22, 25 DGA

After the conditions and processes regarding the registration of recognised data altruistic organisations, Art. 20–22 and Art. 25 DGA deal with their ongoing obligations after their registration. In practical terms, Art. 21 DGA is of central importance here, as it deals with the requirements of actual data processing.

Data altruistic organisations must first fulfil the **transparency requirements** under Art. 20 DGA: This includes keeping a complete and accurate record of all persons who have been given the opportunity to process the data held by this recognised data altruistic organisation, their contact details, the time or duration of the processing or use of the data, the purposes of the processing and any fees paid by the persons processing the data, Art. 20(1) DGA.[1275] In addition, an annual activity report must be published and sent to the competent authority, Art. 20(2) DGA. Further requirements are also mentioned in the recitals.[1276] However, as they have not been included verbatim in the enacting terms of the DGA, some voices in the literature believe that they are not enforceable and legally binding.[1277]

Art. 21 DGA then addresses **the protection and procedural requirements in the interests of data subjects and data holders**.[1278] The regulations are aimed at "protecting the rights and interests of data subjects and data holders"[1279] . Since the GDPR takes precedence with regard to personal data – which must be observed by every recognised data altruism organisation when processing data – the regulatory added value of Art. 21 DGA lies in particular in its provisions for non-personal data.[1280] In principle, personal data processing under the DGA relates to data subjects in accordance with Art. 4 No. 1 GDPR. The processing of non-personal data under the DGA, on the other hand, relates to data holders within the meaning of Art. 2 No. 8 DGA.[1281] According to Art. 21(1) DGA, data altruistic organisations must first inform both data subjects and data holders in a clear and comprehensible manner about the purposes

---

1273 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 19, para. 3.
1274 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 53.
1275 Rachut, S., *ZD* 2024, 248, (249).
1276 Rec. 46 Regulation (EU) 2022/868.
1277 Similarly, Spindler, G., *CR* 2021, 98, (106 et seq.); Tolks, D., *MMR* 2022, 444, (447).
1278 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 66.
1279 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 66.
1280 Paschke, A./Rücker, D./Heckmann, D., DGA, 1st ed. 2024, Art. 21, para. 1; similarly Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 66.
1281 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 66.

of the processing (a) as well as about the location and purposes of general interest in the case of data processing in a third country (b). The principles of altruistic data processing set out in Art. 21(2)–(6) DGA are particularly important. Accordingly, the following principles, among others, must be observed:[1282]

- According to (2), data may only be used together with a specific "purpose"[1283] along the lines of the general interest. It is noteworthy that the DGA does not refer to purposes, as is usual in the GDPR regime. The background or advantage of this somewhat broader term is that altruistic organisations have more leeway when processing non-personal data. [1284]
- According to (2), altruistic data intermediariess may not use **misleading marketing practices**. Misleading is to be interpreted in the sense of the GDPR and the UWG or the relevant case law.[1285]
- Organisations must make it as easy as possible for data subjects and data holders to give and withdraw **consent and permission**, (3).
- Data altruistic organisations must also ensure an **adequate level of security** for the processing of non-personal data, (4). As the GDPR remains applicable, a corresponding obligation with regard to personal data already follows from Art. 32(1) GDPR.[1286] For non-personal data, the DGA leaves a somewhat wider scope for interpretation of what constitutes an adequate level of protection than is provided for in the GDPR.
- Pursuant to (5), data altruistic institutions also have **reporting obligations** towards data holders if an unauthorised transmission or processing of data occurs.[1287] With regard to personal data, Art. 34 GDPR applies without prejudice.

In practice, it is advisable to combine the information obligations from Art. 21(1) DGA and Art. 13 GDPR in a data subject information notice when processing personal data.[1288] When combining the two information obligations, however, care must be taken to ensure that the information does not become confusing and ineffective. This can happen if the information relates to personal and non-personal data.[1289]

The data altruistic organisations must also comply with the provisions of the 'rulebook' issued by the Commission pursuant to Art. 22(1) DGA; the 'rulebook' contains regulations on appropriate information

---

1282 List based on Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 71-77.
1283 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 71.
1284 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 71.
1285 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 73-74.
1286 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 75.
1287 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 76.
1288 A.A. Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 21 para. 53; Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 4 para. 68.
1289 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 21 para. 53.

requirements, suitable technical requirements and security requirements, so-called "communication roadmaps". They also contain recommendations on relevant interoperability standards.[1290]

In order to facilitate the consent of data subjects, which is generally required for data collection, the Commission may draw up a **European data altruism consent form** in accordance with Art. 25(1) DGA in order to ensure that consent and authorisation for altruistic data processing is obtained in a uniform format in all Member States.[1291]

e) Law enforcement: Competent authorities and monitoring practice, Art. 23, 24 DGA

Pursuant to Art. 23(1) DGA, the Member States are obliged to designate one or more competent authorities for data altruistic organisations, whereby these may also be competent authorities for data intermediation services pursuant to Art. 26(1) DGA.[1292]

In the event of violations of the requirements for data altruistic organisations, the competent authority may, pursuant to Art. 24(5) DGA, remove the relevant organisations from the register to be kept pursuant to Art. 17(1) DGA.[1293]

5. Other regulations

In addition to the three major areas of regulation already presented, the DGA also provides for the establishment of a so-called European Data Innovation Board and a comprehensive regulation in the event that the data provided is used in third countries.

a) The European Data Innovation Board, Art. 29 et seq. et DGA

The DGA provides for the Commission to set up a **European Data Innovation Board** (EDIB), which is organised in the form of an expert group.

aa) Organisation of the Data Innovation Board

Members of this body are appointed by the Commission, whereby the DGA does not stipulate a strict, fixed composition, but nevertheless names institutions that must be represented on the Expert Council.[1294] When selecting the members, the focus is particularly on creating a balanced gender ratio and ensuring a geographical balance among the members, Art. 29 p. 2 DGA. In order to ensure that the group functions smoothly and efficiently, an absent or unavailable member is immediately replaced by their deputy.[1295]

The EDIB is divided into at least three subgroups, which are described in more detail in Art. 29(2) DGA and to which different areas of activity are assigned.

1290 Rachut, S., *ZD* 2024, 248, (249).
1291 Tolks, D., *MMR* 2022, 444, (448).
1292 Rachut, S., *ZD* 2024, 248, (249 et seq).
1293 Rachut, S., *ZD* 2024, 248, (250); Tolks, D., *MMR* 2022, 444, (447).
1294 Roth-Isigkeit, D., 'DGA Art. 29' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 3.
1295 Paschke, A./Rücker, D./Keppeler, M./Poncza, M., DGA, 1st ed. 2024, Art. 29 para. 15 et seq.

On the one hand, this includes the subgroup made up of the DGA authorities. On the other hand, a subgroup dealing with technical consultations is planned. The third and final group is for the involvement of stakeholders, including relevant representatives from industry, research, science and third parties.[1296]

The Data Innovation Board itself is supported by a secretariat provided by the Commission, Art. 29(4) DGA. In particular, the secretariat draws up minutes, which are then published in the expert group's register.[1297]

bb) Tasks and responsibilities of the Board

The individual tasks and responsibilities of the EDIB are listed in Art. 30 DGA.

The Council's tasks focus in particular on advising and supporting the Commission in the development of standardised practices and guidelines. For example, according to Art. 30(h) DGA, the Council is authorised to propose guidelines for common European data spaces or to support the creation of sufficient cybersecurity in the exchange and storage of data, Art. 30(e) DGA. In addition, Art. 30(f) and (g) DGA assigns the European Data Innovation Board the task of supporting the development and improvement of standards.[1298] According to Art. 30(i) and (j) DGA, the Innovation Council should also facilitate cooperation between the Member States and the competent authorities by establishing methods for the efficient exchange of information.[1299]

Despite the many different tasks of the Council – the EDIB's remit covers a total of 13 individual tasks – its role is reduced to a purely advisory function; it does not exercise any supervisory powers, nor does it have any legally binding decision-making powers of its own.[1300] As part of its working methods, the European Innovation Council must comply in particular with Art. 12 et seq. Expert Group Decision[1301] and the rules of procedure adopted on the basis of this decision.[1302]

In view of the fact that the provisions of the DGA were kept rather general, the European Data Innovation Board will play a major role in the concrete interpretation and organisation of the regulations.[1303]

1296 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 29 para. 20 et seq.
1297 Paschke, A./Rücker, D./Keppeler, M./Poncza, M., DGA, 1st ed. 2024, Art. 30 para. 28 et seq.
1298 Paschke, A./Rücker, D./Keppeler, M./Poncza, M., DGA, 1st ed. 2024, Art. 30 para. 12.
1299 Paschke, A./Rücker, D./Keppeler, M./Poncza, M., DGA, 1st ed. 2024, Art. 30 para. 23.
1300 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 29 para. 7.
1301 Commission Decision of 30 May 2016 laying down horizontal provisions on the establishment and functioning of Commission expert groups, C(2016) 3301 final.
1302 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 29 para. 16.
1303 Tolks, D., *MMR* 2022, 444, (448); similarly Spindler, G., *CR* 2021, 98, (108).

b) International access and transfer, Art. 31 DGA

Chapter 7 of the DGA creates protection rules if the data provided is to be used in **third countries**. Art. 31 DGA thus regulates the international transfer of non-personal data or international access to such data.[1304] Art. 31 DGA addresses all actors mentioned in the DGA, i.e. public sector bodies, natural or legal persons who have been granted the right to re-use data in accordance with Chapter II, but also providers of data intermediation services and data altruistic organisations.[1305] Objectively, Art. 31 DGA only covers non-personal data; the transmission of personal data is still governed by the GDPR.[1306] As a result, the provisions of the DGA do not overlap here with those of the GDPR on the transmission of personal data to third countries.[1307]

aa) The principle according to Art. 31(1) DGA

Art. 31(1) DGA stipulates that the further processor located in a third country must guarantee the same level of protection for the data concerned as the level of protection guaranteed under EU law.[1308]

In principle, Article 31(1) of the DGA requires all addressees of the DGA to take appropriate technical, legal and organisational measures to prevent the transmission of or access to non-personal data stored in the Union to third countries where such transmission or access would be contrary to Union law or the law of the Member State concerned. Thus, Article 31(1) DGA does not per se prohibit any transmission of non-personal data to third countries.[1309]

However, before the request of an administrative authority of a third country for access to the data of a data holder is complied with, the data holder must be informed in accordance with Art. 31(5) DGA.[1310]

bb) Exceptions to the principle according to Art. 31(1) DGA

An exception to the obligation to prevent international transmissions and access by governmental organisations set out in (1) is found in the cases of Art. 31(2) and (3) DGA.

(1) International agreement pursuant to Art. 31(2) DGA

In the case of Art. 31(2) DGA, compliance with the obligation does not apply because the request for access to data is based on an international agreement, whereby the term international agreement includes, on the one hand, decisions and judgements of a court and, on the other hand, decisions of an

---

1304 This is therefore comparable to the provisions of Chapter V of the GDPR, which only apply to personal data, European Commission, Implementation of the DGA - Guidance, p. 17.

1305 Paschke, A./Rücker, D./Dienst, S./Vogel, P., DGA, 1st ed. 2024, Art. 31 para. 10.

1306 Beyer-Katzenberger, M., 'DGA Art. 31', in: BeckOK Datenschutzrecht, para. 5.

1307 Paschke, A./Rücker, D./Dienst, S./Vogel, P., DGA, 1st ed. 2024, Art. 31 para. 14.

1308 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained (last accessed on: 1 November 2024).

1309 Paschke, A./Rücker, D./Dienst, S./Vogel, P., DGA, 1st ed. 2024, Art. 31 para. 3; European Commission, Implementation of the DGA - Guidelines, p. 17.

1310 European Commission, Implementation of the DGA - Guidelines, p. 18.

administrative authority in third countries.[1311] The existence of a corresponding convention requiring the transmission of data stored in the Union does not exceptionally require that the international transmission or its access be prevented. Art. 31(2) DGA expressly mentions mutual legal assistance agreements, which can therefore be understood as a classic example of corresponding agreements within the meaning of Art. 31(2) DGA.[1312] This refers, for example, to the Agreement between the European Union and the United States of America on extradition and the Council of Europe Convention on Cybercrime of 23 November 2011.[1313]

(2) Comparable rule of law standards pursuant to Art. 31(3) DGA

In the absence of such an agreement, the relevant regulations are set out in Art. 31(3) DGA. Accordingly, the obligation is only waived if the three criteria set out in (3)(a)–(c) DGA are cumulatively fulfilled, which then examine whether or not the rule of law criterion is met in the third country concerned.[1314]

Despite this possible exemption from the obligation under (1), the DGA stipulates that in cases of Art. 31(2) and (3) DGA, the data disclosure must be limited to the minimum – i.e. the smallest possible amount that fulfils the request – Art. 31(4).

6. Supervision, enforcement and sanctions

Art. 34 DGA obliges the Member States to impose sanctions for certain infringements of the provisions of the Regulation in order to ensure the enforcement of the DGA.[1315] In doing so, the legislator has dispensed with sanctions prescribed by EU law and merely regulated the circumstances to which future sanctions are to be linked in order to enforce the law.[1316] However, the national legislator must inform the Commission of the national sanctions packages.[1317] Overall, this gives the Member States a wide margin of discretion in determining their own enforcement criteria.[1318] The list in (1) is exhaustive; accordingly, enforcement provisions are only required for the enumerated offences.[1319] In this respect, Art. 34(1) DGA provides that the respective sanctions must be suitably effective and proportionate as a deterrent. This so-called "minimum triad" can[1320] also be found in other EU legal acts, such as Art. 83(1) GDPR.

1311 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 31 para. 47.
1312 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 31 para. 51.
1313 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 31 para. 51.
1314 Tolks, D., *MMR* 2022, 444, (448).
1315 Schemmel, F., 'DGA Art. 34' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 3; Steinrötter, B./Savary, F., Europäische Plattformregulierung, § 19 para. 77.
1316 Paschke, A./Rücker, D., DGA, 1st ed. 2024, Art. 34 para. 1.
1317 European Commission, Implementation of the DGA Guidelines, p. 19.
1318 Paschke, A./Rücker, D., DGA, 1st ed. 2024, Art. 34 para. 1.
1319 Schemmel, F., 'DGA Art. 34' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 6.
1320 Schemmel, F., 'DGA Art. 34' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 14.

As part of the sanctions, the member states can be guided by the recommendations of the European Data Innovation Board, Art. 34(1) DGA. Art. 34(2) DGA in turn lists the relevant criteria that must be taken into account when imposing the corresponding sanction. These include, for example, the type, severity, scope and duration of the infringement, previous infringements by the provider of data brokering services or the recognised data altruism organisation or other aggravating circumstances in the individual case. The DGA does not specify whether violations of the relevant provisions of the DGA require fault and to what extent intent and negligence are relevant; this area of regulation is also to be defined by the Member States.[1321]

Even if (2) only refers to violations of this regulation, this nevertheless only includes the conclusively regulated violations of the aforementioned articles from (1).[1322]

The addressees of the sanctions will therefore primarily be data intermediation services and data altruistic organisations that have violated the provisions of the DGA.[1323]

Criticism of the sanctions provisions in Art. 34 DGA is particularly fuelled by the fact that the individual sanctions provisions in the member states could diverge and thus stand in the way of the DGA's actual objective of achieving harmonisation.[1324] The legislator was aware of this and expressly recognises this problem in recital 55 of the DGA.[1325] The European Innovation Council was selected as a mediating harmonisation body to counteract the problems arising from this.[1326] Its recommendations are to be taken into account accordingly when determining the sanction provisions to be laid down in the individual Member States. This is intended to prevent excessive differences between the sanctions of the individual member states and, at the same time, to harmonise the sanction regulations.[1327]

The purpose of the provisions of Art. 34 DGA is to motivate players not yet active on the European market to enrich the data economy themselves. Against this background, it is convincing that the regulation largely dispenses with fixed sanctions and leaves a wide margin of manoeuvre to the Member States themselves – after all, new markets cannot be enforced by sanctions.[1328]

Finally, with regard to Art. 34 DGA, it should be noted that the infringements only relate to the provisions of the DGA; other sanction provisions of the member states, such as Art. 83(4) GDPR, remain

[1321] Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 34 para. 9.
[1322] Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 34 para. 22.
[1323] Paschke, A./Rücker, D., DGA, 1st ed. 2024, Art. 34 para. 31.
[1324] Schemmel, F., 'DGA Art. 34' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 4.
[1325] Schemmel, F., 'DGA Art. 34' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 4.
[1326] Schemmel, F., 'DGA Art. 34' in: BeckOK Datenschutzrecht (49th ed. 2024) para. 17.
[1327] Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 34 para. 20; Paschke, A./Rücker, D., DGA, 1st ed. 2024, Art. 34 para. 26.
[1328] Paschke, A./Rücker, D., DGA, 1st ed. 2024, Art. 34 para. 6.

unaffected by Art. 34 DGA.[1329] Sanctioning provisions under competition law are also still applicable in addition to the DGA and remain unaffected, recital 60 DGA.[1330]

Unlike other European legal acts (e.g. Art. 82 GDPR), the DGA does not contain any provisions for **private enforcement**. In the event of breaches of the obligations of the DGA, it is not possible for individuals to claim damages or similar from the relevant bodies. Individuals therefore only have the option of taking action against any infringements in accordance with national law.[1331]

7. Summary and practical implications

Since the publication of the draft regulation, the DGA has faced a wide range of criticism. Insofar as the DGA is viewed in the light of the self-formulated claim of all-encompassing 'data governance', disillusionment initially sets in.[1332] It is true that the DGA recognises the complexity of possible data use in the state, economy and society, which means that it cannot be assigned to any of the traditional areas of law. However, it does not represent the idea of a standardised and, above all, holistic approach to data management regulation, but rather only regulates individual aspects of the data economy in a fragmented manner.[1333]

In general, there is already a lack of reliable evidence to suggest that the low level of activity in the data economy is actually due to a trust deficit, which the DGA is attempting to remedy, and that one of the objectives of the regulation can therefore be achieved at all. Instead, it is more likely that the technical, legal and other obstacles to data trading are holding back the data economy.[1334]

In addition, the effectiveness of the provisions on data altruism (Art. 16–25 DGA) is criticised in the literature. Above all, it is criticised that the regulations on data altruism do not offer sufficient incentives and merely introduce new obligations, for example under Chapter 4 of the DGA, without creating specific grounds for authorisation.[1335] The Commission's power to issue further requirements for data altruistic organisations in accordance with Art. 22 DGA threatens overregulation.[1336] It is also criticised that

1329 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Art. 34 para. 4.
1330 Paschke, A./Rücker, D., DGA, 1st ed. 2024, Art. 34 para. 7.
1331 In Germany, for example, contractual claims for damages can be considered if the obligations of Art. 12 DGA have become part of the licence agreement or competitors can also assert claims under Sections 8 et seq. of the German Unfair Competition Act (UWG) in the event of violations of Art. 11 or 12 DGA. UWG; for detailed information on possible claims under German law, see Hennemann, M./Specht-Riemenschneider, L., HK-DGA, Art. 11 para. 82 et seqq., Art. 12 para. 108 et seqq.; Art. 14 para. 77 et seq.; for detailed information on legal protection for competitors, see Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 6 para. 23 et seqq.
1332 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 4.
1333 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 4 et seq.
1334 Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910); Spindler, G., *CR* 2021, 98, (107) with further references.
1335 Paschke, A./Rücker, D./Heckmann, D., DGA, 1st ed. 2024, Art. 16 para. 53.
1336 Tolks, D., *MMR* 2022, 444, (448).

the DGA in combination with the GDPR does not eliminate existing legal uncertainties, but rather further increases complexity.[1337] Overall, this confirms the impression that the DGA is purely a "marketing measure"[1338]. Truly sustainable effects can only be achieved if the incentives for data altruism are strengthened and the associated obligations are restricted.[1339] However, the introduction of a European model consent form in accordance with Art. 25 DGA, which is designed in compliance with data protection regulations and potentially contributes to the simplification of data altruism, is emphasised positively.[1340]

Another major criticism of the DGA itself is that the far-reaching regulations on data management have not been harmonised with existing data protection regulations. In practice, "incoherent and dysfunctional" results are therefore to be feared.[1341] Legally compliant application of central provisions of the DGA can only take place with constant reassurance of additional data protection guaranteed under the GDPR, which can make practice complex and risky in some cases and not simpler or more innovative, as was actually the aim of the DGA.[1342] This problem was already pointed out during the legislative process, but ultimately only led to minor changes to the original draft regulation.[1343] It should also be criticised that although many of the provisions of the DGA are formulated in great detail, they remain unclear in the end and thus contribute to legal uncertainty**.** The consequence of this is that the actual addressees of the DGA are less concerned with the issue of data usability and do not fully utilise the opportunities offered by the DGA, particularly for fear of violating the existing EU data protection regime.[1344] In addition, the DGA leads to the creation of new authorities, institutions and competences, which leads to demarcation problems with regard to responsibility and can result in overlapping subject areas and uncoordinated, inconsistent decision-making practices.[1345] The DGA does not help to reduce bureaucracy, but rather imposes new bureaucratic obligations on companies.

As a result, it should be noted that, in view of the numerous obligations that the DGA imposes on the addressees, it seems doubtful whether the objective of creating a European data economy has really been advanced or whether, in case of doubt, the opposite has not even been achieved.[1346] In its current form, the DGA is therefore not suitable for achieving all of the aforementioned objectives, which means that it falls considerably short of expectations. The DGA does not currently establish a market, let alone a data economy.

1337 Rachut, S., *ZD* 2024, 248, (252).
1338 In detail Schildbach, ZD 2022, 148, 152.
1339 Steinrötter, D., *DuD* 2021, 794 (798).
1340 Similarly Paschke, A./Rücker, D./Rachut, S., DGA, 1st ed. 2024, Art. 25 para. 79; Rachut, S., *ZD* 2024, 248, (251); in any case Veil, Data Governance Act III: Datenaltruismus, available at: https://www.cr-online.de/blog/2021/10/28/data-governance-act-iii-datenaltruismus/ (last accessed on: 1 November 2024).
1341 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 1 para. 5 et seq.
1342 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 2 para. 75.
1343 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 1 para. 5 et seq.
1344 Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance, § 1 para. 29.
1345 Hennemann, M./Specht-Riemenschneider, L., HK-DGA, 1st ed. 2023, Introduction para. 12.
1346 Similarly Hennemann, M./von Ditfurth, L. *NJW* 2022, 1905, (1910); Tolks, D., *MMR* 2022, 444, (448).

However, it is premature to completely write off the DGA and brand it as a failed regulatory project. As the EU Commission is obliged to evaluate the DGA two years after its entry into force in accordance with Art. 35 DGA[1347], there is reason to hope for an improvement in the legal regulation. Especially as the legal framework that the DGA sets for a flourishing data economy can also be seen as an opportunity for all addressees to contribute to the further development of the internal market.[1348]

[1347] *European Commission*, Implementation of the DGA - Guidelines, p. 19.
[1348] *Schreiber, K./Pommerening, P./Schoel, P., Das neue Recht der Daten-Governance,* § 1 para. 30.

B. Specific part of Data law

I. Sector-specific data access regulations and the concept of European data spaces

Bibliography

Borges, G., & Keil, U. (eds.), Rechtshandbuch Big Data – Grundlagen, Rechtsfragen, Vertragspraxis, 1st ed., Nomos 2023; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Data Strategy, COM(2020) 66 final; European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final; European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2024) 21 final; European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final; European Commission, Proposal for a Regulation of the European Parliament and of the Council on a framework for financial data access and amending Regulations (EU) No. 1093/2010, (EU) No. 1094/2010, (EU) No. 1095/2010, and (EU) 2022/2554, COM(2023) 360 final.

The European Union has rightly recognised that different categories of data differ considerably in their characteristics and therefore also have divergent potential uses and risks – a 'one-size-fits-all approach' to data regulation would therefore be inefficient.[1349] For this reason, the European Commission sees **common European data spaces** as one of the four pillars of the European data strategy.[1350] Data spaces are intended to provide a secure and trustworthy framework for the collection, storage, processing and sharing of data from various sectors and areas of public interest selected by the Commission.[1351] In this way, large, sector-specific data pools are to be created in compliance with data protection and cybersecurity standards, reducing legal and technical barriers to data exchange while taking sufficient account of the sector-specific needs and functioning of certain markets.[1352]

Counterintuitively, the term 'data space' does not always refer to a physical or digital space in which data from certain sectors is collected and made accessible under certain conditions.[1353] The Commission's data strategy, for example, expresses a holistic understanding of the term, according to which common European data spaces are understood as a genuine internal market for data in which data can be used regardless of the physical location of its storage in the Union in compliance with applicable law, which could be of decisive importance for the rapid development of AI technologies, among other things.[1354] At the same time, the term is also used on the one hand abstractly for a concept of data sharing based on sector-specific regulations, and on the other hand concretely for certain applications in practice,

1349 SWD(2022) 45 final, p. 5; COM(2020) 66 final, p. 6.
1350 COM(2020) 66 final, p. 13 et seqq.
1351 SWD(2022) 45 final, p. 2; COM(2020) 66 final, p. 6.
1352 COM(2020) 66 final, p. 25 et seq.
1353 Borges, G./Keil, U., Rechtshandbuch Big Data, sec. 1 para. 77, 78 have identified four different understandings of the term.
1354 COM(2020) 66 final, p. 5; Rec. 2 Regulation (EU) 2022/868.

such as the data space set up by Mobility Data Space GmbH[1355].[1356] What all concepts of data space have in common is that they describe a form of data sharing and joint utilisation within a defined framework. This can be a protected storage location, specific conditions for the shared use of data or specific use cases that are developed on the basis of such regulations.

For the legal sector, the legal framework of common data spaces are of primary interest. In their entirety, they form the **specific part of data law**. The legislator explicitly takes up this distinction between general, horizontal regulations and special, vertical regulations: Art. 1(3)(g) DGA states that the regulation applies to participants in common European data spaces. Art. 30 DGA assigns the European Data Innovation Board the task of submitting guidelines on common European data spaces (h) and supporting the Commission in the development of data spaces (f), (g). Conversely, the legislator expressly states in sector-specific regulations that these are based on the horizontal regulations of the Data Governance Act and the Data Act.[1357]

The definition of certain strategic sectors by the Commission was based on the fact that the use of data in selected areas can have systemic effects.[1358] For this reason, data rooms are planned for the following sectors according to the data strategy:

- Common European **industrial data space** to promote the competitiveness and performance of industry in the EU;
- Common European **data space for the European Green Deal** to promote the use of data to combat climate change;
- Common European **mobility data space** for the development of intelligent transport systems and the consolidation of transport and mobility databases;
- Common European **health data space** to improve data-driven treatments and improve the healthcare system;
- Common European **financial data space** to promote innovation, market transparency and sustainability in the financial sector;
- Common European **energy data space** to support the decarbonisation of the energy system;
- Common European **agricultural data space** to improve the sustainability, performance and competitiveness of the agricultural sector;
- common European **data spaces for public administration** to promote transparency and quality of spending at national and EU level, to simplify law enforcement and to promote technology-enabled governance;

1355 https://mobility-dataspace.eu/de/ (last accessed on: 1 November 2024).
1356 Borges, G./Keil, U., Rechtshandbuch Big Data, sec. 1 para. 78, 79.
1357 See only COM(2022) 197 final, p. 5.
1358 COM(2020) 66 final, p. 25.

- Common European **skills data space** to adapt the education system to the needs of the labour market.[1359]

Finally, a **European cloud for open science** is to be added, which will serve as the basis for a data space for science, research and innovation.[1360] The data strategy published in 2020 already emphasised that the sector list is not exhaustive.[1361] The list has so far been extended to a total of 14 key sectors and now also provides for common European data spaces for the areas of **languages**, **media**, **tourism** and **European cultural heritage**.[1362] The data spaces are then to be gradually linked to form a single European market for data as they are gradually developed.

Various programmes such as **Horizon Europe**[1363] and **Digital Europe**[1364] exist for the concrete implementation of data spaces, which in turn provide for various EU-funded coordination and support measures such as the networking of stakeholders or the provision of technical infrastructure.[1365] In addition, the establishment of shared data spaces is supported by the **Data Spaces Support Centre (DSSC)**[1366], which was founded in 2022.[1367] Furthermore, the Commission has recognised that the coordination and support measures in certain sectors must be accompanied by legislative measures.[1368] The Commission distinguishes between legislative measures that provide for data exchange as a central regulatory instrument and legislative measures that serve to ensure the security, availability and interoperability of data in the private and public sectors.[1369]

The joint data spaces are each at different stages of implementation: while the agricultural data space is scheduled to be operational by the end of 2024, an infrastructure has been under development for the cultural heritage data room since September 2022.[1370] A particular focus here is on 3D digitisation and the improvement of cultural data using artificial intelligence. The energy data space aims to be introduced by 2027 and is supported by standardisation and interoperability projects.[1371] As part of the Horizon Europe funding programme, work is currently underway to provide data for the Green Deal; the first steps should be implemented by 2024.[1372] In contrast, the European Mobility Data Space is due to be launched in 2024 and will provide real-time data on transport and mobility in the Union.[1373] The

1359 COM(2020) 66 final, p. 26.
1360 COM(2020) 66 final, p. 39.
1361 COM(2020) 66 final, p. 27.
1362 For a current list of sectors with specific projects, see https://digital-strategy.ec.europa.eu/de/policies/data-spaces (last accessed on: 1 November 2024).
1363 https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en (last accessed on: 1 November 2024)
1364 https://www.digitaleurope.org/ (last accessed on: 1 November 2024)
1365 SWD(2022) 45 final, p. 8 et seq.
1366 https://dssc.eu/ (last accessed on: 1 November 2024).
1367 SWD(2024) 21 final, p. 11.
1368 COM(2020) 66 final, p. 5.
1369 SWD(2024) 21 final, p. 9.
1370 SWD(2024) 21 final, p. 20.
1371 SWD(2024) 21 final, p. 22.
1372 SWD(2024) 21 final, p. 26 et seq.
1373 SWD(2024) 21 final, p. 36 et seq.

common European data space for public administration comprises several sub-areas such as public procurement and e-government, each of which is to be introduced gradually.[1374]

In the financial sector, the Commission published a legislative package of measures for the digitalisation of the European financial sector in 2023[1375], which includes a proposal for a regulation on access to financial customer data[1376]. The situation is similar in the healthcare sector: due to the global outbreak of the Covid-19 pandemic in 2020, the European health data space was prioritised and a proposal for a regulation on the European health data space was presented.[1377] Both proposals for regulations are presented below.

1374 SWD(2024) 21 final, p. 38 et seqq.
1375 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543 (last accessed on: 1 November 2024)
1376 COM(2023) 360 final.
1377 COM(2022) 197 final.

II. European Health Data Space (EHDS)

Bibliography

Borges, G., & Keil, U. (eds.), Rechtshandbuch Big Data – Grundlagen, Rechtsfragen, Vertragspraxis, 1st ed., Nomos 2023; Denga, M., "Die Nutzungsgovernance im European Health Data Space als Problem eines Immaterialgütermarkts," EuZW (2023), 25; Dettling, H., "Was sind Daten in der Arzneimittelentwicklung und im neuen Datennutzungsrecht (Data Act und European Health Data Space)?" PharmR (2024), 473; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building a European Health Union, COM(2020) 724 final; European Commission, Communication from the Commission to the European Parliament and the Council – A European Health Data Space, COM(2022) 196 final; Forgó, N., "Der European Health Data Space im Kontext der MMR," MMR (2023), 3; Gassner, U., "Forschung und Innovation im europäischen Gesundheitsdatenraum – Zur künftigen Sekundärnutzung elektronischer Gesundheitsdaten," DuD (2022), 739; Hoeren, T., Sieber, U., & Holznagel, B. (eds.), Handbuch Multimedia-Recht, 62nd ed., C.H. Beck 2024; Kühling, J., & Schildbach, R., "Datenschutzrechtliche Spielräume für eine forschungsfreundliche digitale Gesundheitsversorgung – von DS-GVO, SGB etc. zur EHDS-VO und zum GDNG," ZfDR (2024), 1; Petri, T., "Die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten – zum Vorschlag der EU-Kommission für einen Europäischen Gesundheitsdatenraum," DuD (2022), 413; Raji, B., "Datenräume in der Europäischen Datenstrategie am Beispiel des European Health Data Space," ZD (2023), 3; Roos, P., & Maddaloni, J., "Regulierter Datenaustausch zur Gesundheitsforschung," RDi (2023), 225; Taeger, J., & Pohle, T. (eds.), Computerrechts-Handbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 39th ed., C.H. Beck 2024; Werry, S., & Ntanas, E., "Sekundärnutzung von Gesundheitsdaten – Quid deinde?" MMR (2024), 641.

1. Introduction

The global coronavirus pandemic has revealed the shortcomings of European health coordination and highlighted the need for a more harmonised and efficient health strategy. As a result, the European Health Union[1378] was created, the central element of which is the European Health Data Space (EHDS); the European Health Union, in turn, is part of the European Data Strategy.[1379] The proposal for a Regulation on the European Health Data Space[1380] (EHDS-D) aims to create a harmonised legal framework for the exchange of health data across the EU for the purposes of health research and development.[1381] This objective requires standardised legal requirements to lay the groundwork for the production of digital health products and services in the internal market. The EHDS is one of the first sector-specific building blocks in the data strategy concept and thus builds on the horizontal legal acts, namely the Data

1378 COM(2020) 724 final, p. 12 et seq.
1379 COM(2022) 197 final, p. 1.
1380 COM(2022) 197 final.
1381 Rec. 1 EHDS-D.

Governance Act, the Data Act and the requirements of the NIS 2 Directive.[1382] Data security legislation such as the NIS 2 Directive contains provisions that also apply to the healthcare sector.[1383]

a) Legislative procedure

The Commission's draft regulation on the health data space was published on 3 May 2022. The legislative procedure continued until the end of 2023.[1384] Following the Council's compromise proposal 7 December 2023[1385], the European Parliament and the European Council were able to agree on a joint compromise text on 15 March 2024. On 24 April 2024, the Members of the European Parliament then also approved the results of the trilogue.[1386] The final draft is to be submitted to Parliament for vote by the end of 2024. In accordance with Art. 72 EHDS-D, the regulation will enter into force 20 days after publication in the Official Journal of the European Union, i.e. probably in winter 2024.[1387]

At the same time, a set of regulations with a similar objective has already been drafted at national level in Germany with the Health Data Utilisation Act.[1388] This overtook the EHDS in the legislative process and came into force on 31 March 2024.[1389]

b) Goals

According to Art. 1(1) EHDS-D, one objective of the EHDS is to establish a single European health data space, which sets out rules, common standards and procedures as well as infrastructures and a governance framework for the primary and secondary use of electronic health data.

Primary use refers to the use of electronic health data for the provision of healthcare services to assess, maintain or restore the health status of the natural person in accordance with Art. 2(2)(d) EHDS-D; it therefore refers to the processing of data in the direct interest of the data subject. This can be, for example, the prescription of medication.[1390]

According to the legal definition in Art. 2(2)(e) EHDS-D, **secondary use** refers to any processing of electronic health data for other purposes, which are listed in Chapter IV. This refers to data processing

---

1382 COM(2022) 197 final, p. 5.
1383 COM(2022) 197 final, p. 6.
1384 Taeger, J./Pohle, T./Raji, B., European Health Data Space, 120.5 para. 25.
1385 See https://data.consilium.europa.eu/doc/document/ST-16048-2023-REV-1/en/pdf (last accessed on: 1 November 2024).
1386 For the draft in English: https://www.consilium.europa.eu/media/70909/st07553-en24.pdf (last accessed on: 1.11.2024); https://ec.europa.eu/commission/presscorner/detail/de/ip_24_2250 (last accessed on: 1 November 2024).
1387 https://www.bundesgesundheitsministerium.de/themen/internationale-gesundheitspolitik/europa/europaeische-gesundheitspolitik/ehds#:~:text=Die%20EHDS%2DVerordnung%20wird%2020,im%20Herbst%2FWinter%202024%20sein (last accessed on: 1 November 2024).
1388 Werry, S./Ntanas, E., *MMR* 2024, 641 (643).
1389 Art. 6(2) GDNG.
1390 Roos, P./Maddaloni, J., *RDi* 2023, 225 (226).

in the interest of third parties, e.g. for monitoring drug safety (so-called pharmacovigilance) or for developing generative AI models as training data (Art. 34(1)(g) EHDS-D).[1391]

According to the EHDS, the previously fragmented use of health data in the Member States is to be regulated uniformly across Europe in order to enable legal certainty for research on the one hand and to increase patient safety and promote the development of personalised medicine on the other.[1392]

The EHDS is also intended to promote the growth of the digital economy: By creating a single market for digital healthcare products and services, it aims to boost intra-European competition and level the playing field against data-rich foreign big tech companies, which otherwise have an unassailable competitive advantage thanks to their treasure trove of training data.[1393]

Another aim of the EHDS is to strengthen the resilience of healthcare systems across Europe to health crises by developing and harmonising strategies for better crisis preparedness and response across Europe.[1394] The COVID-19 pandemic has also helped to recognise the need for the establishment of a Single Health Data Space.[1395]

c) Structure and systematics of the EHDS

The EHDS is divided into seven chapters, each of which regulates different aspects of the use of electronic health data. Chapter I first defines the scope and the definitions. With regard to the legal terms used in other legal acts, such as data, personal data or health data, the regulation refers to the definitions from the Data Governance Act and the GDPR (Art. 2(2) EHDS-D).[1396] In addition, Art. 2(2) EHDS-D defines which data and systems are covered by the regulation and which actors are affected.

Chapter II deals with the primary use of electronic health data as part of the **MyHealth@EU** initiative.[1397] This concerns the use of this data for the direct benefit of patients, such as for medical treatment and cross-border healthcare within the EU.[1398] This also includes the obligation of healthcare providers to register the processed health data in electronic health records (Art. 7 EHDS-D). The provisions in this chapter are also intended to strengthen the rights of data subjects by giving them simplified access to their health data, regardless of the Member State in which they are located and where they are treated. The declared aim of the EHDS was to give 100% of all EU citizens access to their digital health data by 2023.[1399]

1391 COM(2022) 197 final, p. 4 et seq.
1392 Rec. 1 EHDS-D.
1393 COM(2022) 197 final, p. 2.
1394 COM(2022) 196 final, p. 4.
1395 Rec. 2 et seq. EHDS-D; https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union_de (last accessed on: 1 November 2024).
1396 Dettling, H., *PharmR* 2024, 473 (487), praises the primary use.
1397 https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_de (last accessed on: 1 November 2024)
1398 Rec. 24 EHDS-D.
1399 Rec. 19 EHDS-D.

Chapter III describes the self-certification process and the requirements for electronic health record systems (EHR systems) in detail. Both the legal and technical requirements for ensuring the interoperability and data security of these systems are defined. Chapter IV then deals with the permitted uses of electronic health data for secondary purposes and at the same time specifies which uses are not permitted. This serves to clearly delineate authorised and prohibited applications in the context of data law.

Chapter V is dedicated to additional measures that are necessary to ensure capacity building and the secure flow of data to third countries. This chapter also describes technical and organisational precautions that are essential for the protection of data and the smooth operation of the systems.

The establishment and tasks of the European Health Data Space Committee are explained in Chapter VI. Art. 64 et seq. EHDS-D. They regulate in particular the coordination and cooperation of the Committee with national authorities in order to ensure uniform implementation of the regulations.[1400]

Finally, Chapter VII deals with the European Commission's power to adopt delegated acts in order to specify detailed issues of the European Health Data Space (EHDS). This delegated legislative competence enables the Commission to react in a targeted manner to developments in implementation and to make necessary adjustments in order to prevent undesirable trends at an early stage.[1401]

2. Rights and obligations of the parties involved

The actors involved and their rights and obligations differ depending on the type of data utilisation. The rights and obligations of the persons involved are therefore presented below according to primary and secondary use.[1402]

a) Primary use of electronic health data

The **primary use of electronic health data** is legally defined in Art. 2(2)(d) EHDS-D and refers to the processing of electronic health data for the provision of healthcare services to assess, maintain or restore the state of health of the natural person to whom the data relates, including the prescription, dispensing and provision of medicinal products and medical devices, as well as for the relevant social security, administrative or reimbursement services. Primary use starts with the initial collection of health data, which in practice is likely to be carried out regularly by a doctor who, for example, takes MRI images of the patient as part of the diagnostic process.[1403] Data can also be collected by the data subject themselves, for example by measuring their heart rate using a wearable device.[1404] Those individuals who collect the data for the first time are referred to as **health data holders.** Art. 2(2)(y) EHDS-D defines

1400 Rec. 42 EHDS-D.
1401 Rec. 68 EHDS-D.
1402 Hoeren, T./Sieber, U./Holznagel, B/Wehde, A./Brandenberg, J., Handbuch Multimedia-Recht, Part 16.8 para. 6, 7.
1403 Hoeren, T./Sieber, U./Holznagel, B/Wehde, A./Brandenberg, J., Handbuch Multimedia-Recht, Part 16.8 para. 8.
1404 Hoeren, T./Sieber, U./Holznagel, B/Wehde, A./Brandenberg, J., Handbuch Multimedia-Recht, Part 16.8 para. 8.

health data holder as a natural or legal person who is an organisation or entity in the health sector, in the social security sector, in the care sector or in the area of reimbursement services, or who carries out research activities in relation to these sectors, as well as Union institutions, bodies, offices and agencies which are subject to this Regulation, applicable Union law or national law implementing Union law. These can therefore be both public and private organisations in the health and care sector.[1405] By contrast, a **user of health data** (Art. 2(2)(z) EHDS-D) is a natural or legal person or a Union institution, body, office or agency that has been lawfully granted access to electronic health data for secondary use in accordance with this Regulation on the basis of a data authorisation or a request for health data.

Access to and transmission of personal electronic health data for primary use is regulated in Art. 3 et seq. EHDS-D.

The trilogue draft now contains a detailed catalogue of rights of natural persons in Art. 8(a) – (h) EHDS-D, which are very similar in content to the rights of data subjects already known from the GDPR. For example, according to Art. 8a(2) EHDS-D, the data subject has the right to receive a copy of their electronic health data for their electronic patient file.

At this point, reference should also be made to the MyHealth@EU initiative. In accordance with Art. 12 EHDS-D, this is a digital infrastructure for cross-border access to electronic health data, which is intended to enable cross-border access to electronic health data. This is also to be achieved by connecting the national **eHealth contact points** to a central platform.[1406]

The initiative promotes two main purposes: Firstly, it should enable natural persons to redeem prescriptions in other EU countries in accordance with Art. 12(6) EHDS-D. In addition, according to Art. 13(1) EHDS-D, a digital patient file should be able to provide treating physicians with important information in their own language.[1407] By making health data available across national borders, EU citizens should be able to receive treatment in hospitals, medical practices or other facilities throughout the EU without any differences in the quality of treatment.

While the digital registration of health data in the EDHS is mandatory, the Member States can use the opening clause in Art. 8h EHDS-D to provide a right of objection for primary use at national level. The opt-out options provided for in the German DigiG therefore remain in place.[1408]

b) Secondary use of electronic health data

According to Art. 2(2)(e) EHDS-D, the **secondary use of electronic health data** is the processing of electronic health data for the purposes of Chapter IV. The data used may include personal electronic

1405 Rec. 40 EHDS-D.
1406 Rec. 24, 25 EHDS-D.
1407 Taeger, J./Pohle, T./Raji, B., European Health Data Space, 120.5 para. 23.
1408 https://www.bundesgesundheitsministerium.de/themen/internationale-gesundheitspolitik/europa/europaeische-gesundheitspolitik/ehds (last accessed on: 1 November 2024).

health data initially collected for primary use as well as electronic health data collected for the purposes of Chapter IV of this Regulation.

The access procedure for enabling the secondary use of electronic health data is standardised in Art. 45 et seq. EHDS-D.[1409] The applicant submits an application to the access point, which then reviews the application and, if the outcome of the review is positive, grants access to the data owner. Whether an **applicant** (Art. 2(2)(z), (a) EHDS-D) is granted the so-called **health data authorisation** (Art. 2(2)(aa) EHDS-D), in other words whether data access is granted, is decided by the **access points for health data** in accordance with Art. 37(1)(a), Art. 46 EHDS-D.[1410]

As a rule, the health data must be released in anonymised form.[1411] However, if this would defeat the purpose of use, the data can also be shared in pseudonymised form.[1412] The pseudonymisation key is kept by the access point; re-identification by the data user is punishable by law (Art. 41a(2a) EHDS-D in conjunction with Art. 43a(5c) EHDS-D).

The secondary use of electronic health data is only permitted if one of the purposes listed enumeratively in Art. 34(1) EHDS-D is fulfilled. These include

- activities for reasons of public interest in the field of public health and occupational health, e.g. protection against serious cross-border threats to health, monitoring public health or ensuring high standards of quality and safety of healthcare, medicinal products or medical devices (a);
- assistance to public sector bodies or Union institutions, bodies, offices and agencies, including regulatory authorities, in the health or care sector in the fulfilment of their tasks as defined in their mandates (b);
- compilation of official statistics on the health or care sector at national, multinational and Union level (c);
- educational or teaching activities in the health or care sector (d);
- scientific research in the health or care sector (e);
- development and innovation activities for products or services that contribute to public health or social security or ensure high quality and safety standards for healthcare, pharmaceuticals or medical devices (f);
- training, testing and evaluation of algorithms, including in medical devices, AI systems and digital health applications that contribute to public health or social security or ensure high quality and safety standards for healthcare, medicinal products or medical devices (g);
- provision of personalised healthcare where the health status of a natural person is assessed, maintained or restored on the basis of the health data of other natural persons (h).

1409 For detailed information on the access procedure based on the Commission's draft Hoeren, T./Sieber, U./Holznagel, B/Wehde, A./Brandenberg, J., Handbuch Multimedia-Recht, part 16.8 para. 22.
1410 Borges, G./Keil, U., Rechtshandbuch Big Data, sec. 1 para. 85.
1411 Rec. 49 EHDS-D.
1412 Rec. 49 EHDS-D.

If the secondary use fulfils one of the prohibited purposes set out in Art. 35 EHDS-D, access to the data will be denied.

The Commission's draft envisaged secondary use without consent, i.e. no involvement of the data subjects. Some saw this as an unjustified restriction of data subjects' rights and informational self-determination.[1413] The compromise text between the Council and Parliament then included the option for natural persons to **object** to the secondary use of their electronic health data (**opt-out**).

According to Art. 35f(1) EHDS-D, natural persons now have the right to withdraw their consent to the secondary use of their data at any time and without giving reasons.

According to Art. 35f (2) EHDS-D, the Member States are obliged to establish an accessible and easily understandable objection procedure for natural persons. However, under strict conditions, Art. 35f(3) EHDS-D allows for an exception to the opt-out mechanism to be established at Member State level, thus allowing for a return to the consent-free secondary use from the Commission draft, provided that the use of the data is in the particular public interest (Art. 34 (1)(a) – (c) EHDS-D).

3. Supervision , enforcement and sanctions

Pursuant to Art. 69 EHDS-D, the Member States are obligated to implement legal provisions for the enforcement of penalties for violations of the EHDS. Art. 69(a) – (f) EHDS-D contains the criteria to be taken into account by the Member States during the assessment of infringements. These criteria include the duration and effects of the infringement, as well as the obtaining of a financial advantage through non-compliance with the provisions. This option was already included in the Commission draft.

What is new, however, is a separate legal basis for the imposition of fines in Art. 43a EHDS-D. In terms of content and structure, this in turn is very similar to the sanction mechanism known from antitrust law and the GDPR, which provides for a fine of 10,000,000 euros or 2% or 20,000,000 euros or 4% of the previous year's global revenue, depending on the severity of the offence.

The trilogue version now also contains a horizontal complaints mechanism for the first time in Art. 68a EHDS-D, with which data subjects can initiate an investigation by the supervisory authority in the event of a violation of their rights under the EHDS.

In addition, Art. 43 EHDS-D also enables supervisory authorities to impose fines, revoke granted data access or entirely exclude actors from secondary use for a duration of up to 5 years in the instances of persistent violations.

[1413] Cf. Raji, B., *ZD* 2023, 3 (7); Petri, T., *DuD* 2022, 413 (418); see also Kühling, J./Schildbach, R., *ZfDR* 2024, 1 (18).

Finally, Art. 69a EHDS-D provides natural persons with a right to compensation for material or non-material damage caused by violations of the provisions of the EHDS. However, it is unclear to what extent this competes with the identical basis for claims under Art. 82 GDPR.

4. Summary and practical implications

Firstly, it should be noted that the 2024 draft of the EHDS changes the date of individual provisions. In some cases, the date was shortened by one year, for example with regard to the date of Art. 70(1) et seq. EHDS-D.[1414]

The failure to determine the scope of the possibilities of commercial health research should also be viewed critically.[1415] Furthermore, the interactions with other legal acts of data law and competition law in particular remain unclear.

The relationship with data protection law is equally difficult.[1416] According to recital 25 EHDS-D, the provisions of the EHDS should follow and comply with data protection regulations. However, the secondary use of electronic patient records is difficult to reconcile with the purpose limitation principle.[1417] Although the opening clause in Art. 89 GDPR allows the purpose limitation principle in Art. 5 GDPR to be relaxed, the scope of the EHDS is likely to be broader than that of the research clause under the GDPR.[1418] In addition, there are difficulties with regard to the requirement of accuracy or the right to rectification in the case of the mass collection of health data, especially if this data originates from fitness trackers or smartwatches, for example. Especially when this data is also processed by AI-based algorithms, it is almost impossible to create the necessary transparency for the data subject. Finally, it seems questionable how the requirements of the EHDS can be met and how sufficient anonymisation can be ensured over time. Although the access points should ensure that health data is sufficiently anonymised when it is made available for secondary use in accordance with Art. 44(1) EHDS-D, this is not always possible, especially in the case of rare diseases or genetic data, due to its individuality and immutability.[1419]

Questions of antitrust law also remain unresolved: recital 75 EHDS-D emphasises that the application of competition law, in particular Art. 101, Art. 102 TFEU, remains unaffected and that the planned measures must not restrict competition. In this light, however, the question arises as to whether the withholding of health data, which is permitted under Art. 43(5) EHDS-D, could not also constitute an abuse of a dominant market position under Art. 102 TFEU. This in turn raises questions about the relationship between cartel authorities and access points. It also appears questionable whether the data obtained by the data holders does not allow conclusions to be drawn about production costs and profit

1414 Cf. II. 11. f) of the introduction to the compromise of the EHDS-D.
1415 Gassner, U., *DuD* 2022, 739 (742) et seq.; Roos, P./Maddaloni, J., *RDi* 2023, 225 (230).
1416 Forgó, N., *MMR* 2023, 3 (4).
1417 Raji, B., *ZD* 2023, 3 (7).
1418 Denga, M., *EuZW* 2023, 25 (30), is already critical overall.
1419 Denga, M., *EuZW* 2023, 25 (30).

margins, which could lead to collusive behaviour in accordance with Art. 101(1)(a) TFEU and thus also facilitate an infringement of competition law.

The protection of electronic health data containing intellectual property and trade secrets of private companies is guaranteed by Art. 33a EHDS-D. In principle, this data should also be made available for secondary use. However, all necessary measures must be taken to protect the confidentiality of intellectual property rights and trade secrets. However, the European legislator leaves open what exactly is meant by "all necessary measures", which in turn can lead to application problems in practice.[1420] Under the Commission's draft, the protection of intellectual property was still solely in the hands of the access point.[1421] In the trilogue text, a right to refuse access has now been established for exceptional cases where there is a significant risk that cannot be satisfactorily mitigated by contractual obligations or technical measures, for example.[1422]

[1420] Dettling, H., *PharmR* 2024, 473 (488), is similarly critical.
[1421] Roos, P./Maddaloni, J, *RDi* 2023, 225 (229).
[1422] Art. 33a(1)(d) EHDS-D.

III. Financial Data Access Regulation (FiDAR)

Bibliography

Awrey, D., & Macey, J., "The Promise & Perils of Open Finance," *Yale Journal on Regulation*, Vol. 40 (2023), 1–60; Dreisigacker-Sartor, C., & Ritter-Döring, V., "Mit FIDA von Open Banking zu Open Finance," *RdZ* (2024), 5; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European Data Strategy, COM(2020) 66 final; European Commission, Impact Assessment Report – FIDA, SWD(2023) 224 final; Gesamtverband der Versicherer (GDV), Stellungnahme des Gesamtverbandes der Deutschen Versicherungswirtschaft zum FIDA-E v. 28.7.2023, accessible at: https://www.gdv.de/resource/blob/138620/a775377b333d48e7b4ebe4aaffe856b1/fida-data.pdf; Izzo-Wagner, A., Otto, T., & Schultess, P., "Der Entwurf eines EU-Frameworks for Financial Data Access," *RDi* (2024), 11; Mayer, P., "Ein offenes Finanzwesen für Europa – Der Zugang zu Finanzdaten nach dem Kommissionsentwurf der Financial Data Access Regulation (FIDAR)," *ZdiW* (2023), 258; Vig, Z., "Der Kommissionsentwurf für die Verordnung über den Zugang zu Finanzdaten," *BKR* (2023), 659; Zahrte, K., "Das Financial Data Access and Payments Package Teil I: PSD 3 und PSR," *ZIP* (2023), 2555; Zahrte, K., "Trends im Zahlungsdiensterecht Teil II: FiDA, Digitaler Euro und Bargeldregulierung," *ZIP* (2024), 542.

1. Introduction

The fourth pillar of the European Union's data strategy consists of the concept of "common European data spaces in strategic sectors and areas of public interest"[1423]. In particular, this involves the creation of sector-specific regulations to supplement the horizontal legal acts adopted as part of the data strategy. The European financial sector discussed here was considered on 28 August 2023 with the draft regulation on the access to financial data ('Financial Data Access Regulation'[1424], hereinafter: FiDAR-D).

In almost every industry, customer data gives companies a significant competitive advantage over rival market players, so many companies are unlikely to have a genuine self-interest in sharing data with their competitors; this market situation can also be found in the financial sector.[1425] However, this situation represents an obstacle to the utilisation of data for the benefit of the (European) community.[1426] Therefore, the aim of FiDAR is to break down the data silos held by companies in the financial sector and make this data accessible in the interests of customers and third parties.[1427]

1423 COM(2020) 66 final.

1424 Proposal for a Regulation of the European Parliament and of the Council on a framework for access to financial data and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554, COM(2023) 360 final.

1425 Awrey, D./Macey, J., 40 *Yale J. on Reg*. 2023, 1 (3).

1426 Zahrte, K., *ZIP* 2024, 542.

1427 Rec. 3, 6 et seq. FiDAR-D; Mayer, P., *ZdiW* 2024, 258 (259).

According to the Commission's vision, FiDAR is intended to further develop the 'open banking' concept introduced under PSD2[1428] into the so-called 'open finance'.[1429] **Open Banking** refers to the access to payment account data to be granted by financial institutions for payment initiation services and account information services in accordance with PSD2.[1430] In contrast, **Open Finance** goes further, as FiDAR is now intended to make other financial data usable for customers in addition to account data.[1431] Usability in this sense means, in particular, the possibility for customers to pass on their financial data to '**third-party providers'** (TPPs).[1432] This should enable innovative and customised financial products and services to be offered to customers, which in turn will increase competition between companies in the financial sector.[1433]

2. Scope, Art. 2 FiDAR-D

From a factual perpective, the scope of the FiDAR-D encompasses specific categories of customer data, Art. 2(1) FiDAR-D. According to the definition in Art. 3 No. 3 FiDAR-D, customer data is defined as all data that is typically collected, stored and processed by financial institutions in the course of their standard business operations with customers, regardless of whether it constitutes personal data or non-personal data such as financial product characteristics. According to the FiDAR-D, the categories of user data covered pursuant to Art. 2(1) FiDAR-D are as follows:

- Mortgage credit agreements, loans and accounts (a), with the exception of payment accounts, which are covered by PSD2 ,[1434]
- Savings, investments in financial instruments, insurance investment products, crypto assets, real estate and other related financial assets and the economic benefits of these assets; including data collected for the assessment of suitability and appropriateness in accordance with Art. 25 MiFID-II[1435] (b),
- Pension entitlements from company pension schemes in accordance with the IORP II Directive[1436] and the Solvency II Directive[1437] (c),

---

1428 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC, OJ L 337/35 (PSD2).

1429 Dreisigacker-Sartor, C./Ritter-Döring, V, *RdZ* 2024, 5 (5) et seq.; *Mayer*, ZdiW 2024, 258.

1430 Dreisigacker-Sartor, C/Ritter-Dörung, V, *RdZ* 2024, 5 (6); Zahrte, K., *ZIP* 2023, 2555 (2558) et seq.

1431 Awrey, D./Macey, J., 40 *Yale J. on Reg*. 2023,1 (4); Dreisigacker-Sartor, C./Ritter-*Dörung*, V., *RdZ* 2024, 5 (7).

1432 Mayer, P., *ZdiW* 2024, 258.

1433 Rec. 2, 3, 15 FiDAR-D; Mayer, P., *ZdiW* 2024, 258.

1434 Mayer, P., *ZdiW* 2024, 258 (263); Zahrte, K., *ZIP* 2024, 542 (543).

1435 Directive (EU) 2014/65 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments. OJ L 173/349.

1436 Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs), OJ L 354/37.

1437 Directive (EC) 2009/138 of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), OJEU No. L 335.

- Pension entitlements from pan-European private pension products in accordance with the PEPP Regulation[1438] (d),
- Non-life insurance products in accordance with the Solvency II Directive, with the exception of health insurance products; including data collected to determine the wishes and needs of the customer in accordance with Art. 20 IDD[1439] , as well as data collected to assess suitability and appropriateness in accordance with Art. 30 IDD (e),
- Data collected to assess the creditworthiness of a company in the context of a credit application procedure or an application for a credit assessment (f) and
- non-sensitive data categories used by data holders to fulfil the know-your-customer compliance requirements[1440] of business customers (fa)

The personal scope includes the groups of persons specified in Art. 2(2) FiDAR-D.[1441] These include credit institutions, payment institutions, e-money institutions, providers of crypto services and financial information service providers.[1442] These persons assume the role of either data holder or data user in a triangular relationship, Art. 3 No. 5 and 6 FiDAR-D.[1443] In contrast, the customer is defined in Art. 3 No. 2 FiDAR-D.[1444]

According to Art. 3 No. 5 FiDAR-D, data holders are financial institutions that collect and store one or more of the data categories listed in Art. 2(1) FiDAR-D. This definition covers almost all financial services.[1445]

According to Art. 3 No. 6 FiDAR-D, data users are those entities listed in Art. 2(2) FiDAR that have lawful access to the customer data listed in Art. 2(1) FiDAR with the customer's authorisation. It is evident that this also covers practically all financial service providers, as a non-data-based business model is only likely to occur in isolated cases.[1446]

It is stated in Art. 3 No. 2 FiDAR-D that the term 'customer' is to be understood as a natural person residing within the Union, or a legal person established within the Union who is a consumer or a micro,

1438 Regulation (EU) 2019/1238 of the European Parliament and of the Council of 20 June 2019 on a Pan-European Private Pension Product (PEPP), OJ L 198/1.
1439 Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution, OJ L 26/19.
1440 The know-your-customer principle refers to Art. 8 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 141/73.
1441 Izzo-Wagner, A./Otto/Schultess, P., *RDi* 2024, 11 (14).
1442 For a complete list, see Mayer, P., *ZdiW* 2024, 258 (260).
1443 Vig, S., *BKR* 2023, 659 (660).
1444 Mayer, P., *ZdiW* 2024, 258 (261).
1445 Vig, S., *BKR* 2023, 659 (660).
1446 Vig, S., *BKR* 2023, 659 (660) et seq.

small or medium-sized enterprise (SME) that is a party to an agreement on the use of financial products and services or has requested such an agreement.

3. Data access claims, Art. 4–7 FiDAR-D

In Articles 4–7, FiDAR-D regulates the customer's statutory right to access their own financial data as well as the data access of other service providers to the customer's financial data at the customer's request. The fulfilment of the data access right by the data holder requires an electronic request either by the customer himself or on his behalf, Art. 4, 5(1) FiDAR-D.[1447]

a) Access by the customer, Art. 4 FiDAR-D

First and foremost, the data holder's obligation under Art. 4 FiDAR-D must be mentioned, according to which access to the collected financial data must be granted at the customer's request.[1448] In doing so, the data holder must ensure certain formal requirements: The data must be made available via an application programming interface (API) accessible to the customer in an easily readable format. The presentation of the data should reflect the state in which the data is available to the data owner at the time the customer requests access. In addition, data retrieval must be possible without undue delay, free of charge, continuously and in real time.

b) Access by a data user, Art. 5 (1) FiDAR-D

FiDAR is intended to give data users with the express permission of the customer the opportunity to offer the customer personalised financial services.[1449] The use cases listed by the Commission include financial management tools, more efficient investment advice and credit checks when financing SMEs.[1450] In order to enable such and other services from third-party providers, Art. 5(1) FiDAR-D stipulates that the data holder must grant a data user acting on behalf of the customer access to the customer's financial data. This requires an explicit request from the customer and the customer's explicit consent to the use of their data, which is carried out by the customer via a special online or mobile customer interface. The data transmission to the data user must then take place without undue delay, continuously and in real time.

In order to alleviate the financial and technical costs associated with maintaining the data access infrastructure the data holder is granted the option to do so under Art. 5(2) FiDAR-D to impose a charge on the data user for data access in accordance with the boundary conditions outlined in Art. 9, 10 or 11 FiDAR-D.[1451]

1447 Dreisigacker-Sartor, C./Ritter-Dörung, V., *RdZ* 2024, 5 (8); Mayer, P., *ZdiW* 2024, 258 (263).
1448 Dreisigacker-Sartor, C./Ritter-Dörung, V., *RdZ* 2024, 5 (8).
1449 Rec. 2 FiDAR-D.
1450 SWD(2023) 230 final, p. 118 ff; Mayer, P., *ZdiW* 2024, 258 (262) et seq.
1451 Rec. 23 FiDAR-D; Dreisigacker-Sartor, C./Ritter-Dörung, V., *RdZ* 2024, 5 (9).

According to Art. 6(1) FiDAR-D, only those data users who are financial institutions within the meaning of Art. 3 No. 8 FiDAR-D or who are authorised as financial information service providers pursuant to Art. 14 FiDAR are able to obtain data access within the meaning of Art. 5 FiDAR-D.[1452]

c) Authorisation dashboard, Art. 8 (1) FiDAR-D

Data holders are obliged to provide the customer with so-called **authorisation dashboards**, Art. 8(1) FiDAR-D. These should be user interfaces that enable the customer to manage all of their authorisations granted to data users.[1453] According to Art. 8(2)(a) FiDAR-D, the dashboard must contain the following information regarding each current authorisation in an easily understandable manner and to the extent available to the data owner:

- The name of the data user to whom access was granted (i);
- the customer account, financial product or financial service to which access has been granted (ii);
- the purpose of the authorisation (iii);
- the categories of data to which access has been granted (iv);
- the period of validity of the licence (v);
- the dates on which the data was accessed (vi).

The input screen must therefore offer the option of limiting or withdrawing consent and restricting it to certain purposes of use.[1454]

4. Data sharing systems, Art. 9–11 FiDAR-D

Art. 9–11 FiDAR-D provide for a common system for access to financial data. Data users and data holders should belong to these systems in order to standardise contractual and technical interaction in the internal market and thereby increase the efficiency of data access.[1455]

However, according to Art. 10(1)(a) FiDAR-D, only data users and data holders who control a significant part of the market, as well as consumer associations and customer organisations, are obliged to belong to a system. There is no guidance yet on how to determine when control of a significant part of the market is given.[1456]

A data sharing system consists of collective contractual agreements between data holders and data users.[1457] The proposal does not rule out the possibility of a system being realised in the form of a company or association.[1458] FiDAR will provide for deadlines by the end of which data holders and data users

1452 Mayer, P., *ZdiW* 2024, 258 (263); Vig, S., *BKR* 2023, 659 (662).
1453 Rec. 21 FiDAR-D.
1454 Vig, S., *BKR* 2023, 659 (661).
1455 Rec. 25, 26 FiDAR-D.
1456 Mayer, P., *ZdiW* 2024, 258 (262) et seq.
1457 Rec. 26 FiDAR-D; Mayer, P., *ZdiW* 2024, 258 (263).
1458 Vig, S., *BKR* 2023, 659 (662).

must be participants in at least one financial data access system, Art. 9(1)(2) FiDAR-D. The competent national supervisory authority must also be informed of the systems to which a data holder belongs, Art. 10(3) FiDAR-D.

A financial data access scheme must regulate at least the points specified in Art. 10 No. 1 FiDAR-D. This includes, in particular, provisions on the requirements for membership (b) and (c), on the common standards and norms for interfaces and data (g), on the remuneration model pursuant to Art. 5(2) FiDAR-D (h), on the contractual liability of members (i) and on a dispute resolution procedure (j) as well as a mechanism for compensating customers in the event of data loss, damage or fraud (ia).

If no or inadequate financial data access systems have been developed by the deadline, the European legislator reserves the right to supplement FiDAR with corresponding provisions in Art. 11 FiDAR-D. Primarily, however, the development of the systems is envisaged to be carried out by its members, if necessary with the support and involvement of the authorities, Art. 11(1) FiDAR-D.

5. Summary and practical implications

The implementation of the FiDAR regulations will not be possible without a certain investment on the part of the data holders.[1459] It remains to be seen whether the benefits for customers, data users and ultimately the entire market can justify these costs. The amendments made in the first reading in the European Parliament on 30 April 2024 already show that the legislator is addressing the criticism of the draft and further specifying the provisions.[1460] It is also positive that the draft also takes into account special circumstances, such as the possibility of setting up a common interface for SMEs.[1461] With Art. 9(1a) FiDAR-D, the legislator also takes account of requests for a staggered implementation of the financial access systems.[1462]

In this respect, the willingness of the regulators to take into account the position of the various key players is cause for optimism. FiDAR is therefore already emerging as an important step on the promised path from open banking to open finance.[1463]

1459 GDV, Statement of the German Insurance Association on the FIDA-E, 2023, p. 7.
1460 Izzo-Wagner, A./Otto, T./Schultess, P., *RDi* 2024, 11 (18); Mayer, P., *ZdiW* 2024, 258 (268) et seq.
1461 Rec. 23 FiDAR-D.
1462 BR-Drs. 429/23 No. 2; GDV, Statement of the German Insurance Association on the FIDA-E, 2023, p. 3 et seq.
1463 Vig, S., *BKR* 2023, 659 (664).

Chapter 3: Regulation of data-based business models

Literature

Azkan/Goecke/Spiekermann, Forschungsbereiche der Datenökonomie, Wirtschaftsdienst 2020, Heft 2, p. 124; *Borges/Keil*, Rechtshandbuch Big Data, 1st edition; *Brown et. al*, Language models are few-shot learners, Advances in Neural Information Processing Systems, Vol. 33 (2020), pp. 1877 - 1901; *Drewes/Meyer/Moss*, Update: Europäische Plattformregulierung - Die ersten Schritte von DMA und DSA in der Praxis, RDi 2024, 310; *Fries/Scheufen*, Märkte für Maschinen, MMR 2019, 721; *Hessel/Leffer/Potel*, Datengetriebene Geschäftsmodele, ZD 2022, 537; *Höppner*, Plattform-Regulierung light, WuW 2020; *Lennartz*, Digitale Puppenspieler - die Nachbildung von Körper und Stimme durch KI NJW 2023, 3543; *Martini/Drews/Seeliger/Weinzierl*, Dark Patterns, ZfDR 2021, 47; *Paal/Hüger*, Die KI-VO und das Recht auf menschliche Entscheidung, MMR 2024, 540; *Rhode et. al*, Datenwirtschaft und Datentechnologie, 1st edition, Berlin 2022; *Schneidereit*, Auswirkungen des Data Act auf innovative datengetriebene Geschäftsmodelle in der Medizintechnik, CR 2023, 9; *Wagner/Eidenmüller*, In der Falle der Algorithmen? Skimming off consumer surplus, exploiting behavioural anomalies and manipulating preferences: Regulating the dark side of personalised transactions, ZfPW 2019, 220.

Data-based business models have become a key driver of the global economy in recent years.[1464] Such business models are characterised by the fact that they focus on the systematic use of data to create added value and new business opportunities.[1465] In short, this is the value-generating use of data.[1466] Large amounts of data are collected, analysed and used to optimise decisions, develop innovative products or make business processes more efficient. A prominent example of innovative data-based products are so-called **Large Language Models (LLM)**, which are used in chatbots such as '**ChatGPT**'[1467] or '**Gemini**'[1468] and are trained with text data of over 570 gigabytes, although the total amount of unstructured data can be significantly larger.[1469] Data for **networked products** such as smartphones, vehicles or industrial machines that are connected to the Internet and continuously collect and analyse data in order to make their functionality and interactivity more efficient is no less important.[1470] In the area of **online platforms**, data is collected, analysed and monetised in a targeted manner by using it to personalise content and target advertising.[1471] At the same time, platforms use the aggregated data to optimise their algorithms and recommendations, which increases user loyalty and at the same time enables higher advertising revenue.[1472] Last but not least, data-based business models have also become established in

---

1464 For Germany, for example, see *Fritsch/Krotova*, Wie datengetrieben sind Geschäftsmodelle in Deutschland? - Analysing the status quo, IW Report 09/20, p. 3.

1465 *Rohde/Bürger/Peneva/Mock*, Data Economy and Data Technology, p. 1 et seq.

1466 *Azkan/Goecke/Spiekermann*, Wirtschaftsdienst 2020, 124, 125.

1467 https://openai.com/index/hello-gpt-4o/ (last accessed on: 1 November 2024).

1468 https://blog.google/technology/ai/google-gemini-ai/#introducing-gemini (last accessed on: 1 November 2024).

1469 The figures apply to the GPT-3 model, *Brown et. al*, 33 Adv. Neural Inf. Process. Syst. (2020), 1877, 1885.

1470 *Borges/Keil/Maaß*, Rechtshandbuch Big Data, Section 2 para. 34 ff; *Schneidereit*, CR 2023, 9 et seq.; *Fries/Scheufen*, MMR 2019, 721, 722.

1471 *Hessel/Leffer/Potel*, ZD 2022, 537.

1472 *Drewes/Meyer/Moss*, RDi 2024, 310; *Höppner*, WuW 2020, 71.

e-commerce - companies use the extensive customer, transaction and behavioural data available to develop personalised recommendations, targeted advertising and dynamic pricing strategies.[1473]

In addition to the enormous value creation potential of data-based business models, this can also pose considerable risks for users of AI applications, connected products and online platforms: Online platforms and marketplaces can also use their data collections, among other things, to create personalised offers and recommendations that influence the consumer behaviour of their users and encourage them to make purchasing decisions through algorithmically controlled stimuli, so-called **dark patterns.**[1474] Apart from the obvious conflict with the fundamental right to informational self-determination, such practices are also in conflict with users' private autonomy.[1475] In addition, so-called **deepfakes**, which are deceptively real media content of a person or event created with the help of artificial intelligence and pose a risk to the personal rights of the persons concerned by being used for disinformation, damage to reputation or other abusive purposes without the consent of the person concerned, are increasingly circulating on the internet and on social media in particular.[1476] Finally, the mass use of data-driven AI-based applications, which often involve non-transparent and difficult-to-understand decision-making processes, raises questions about accountability and control over algorithmic decisions.[1477]

The risks outlined here only vaguely illustrate that data-driven business models are not only characterised by their potential for growth and innovation, but also pose a real threat to the fundamental rights of the people who come into contact with them. The European Commission has recognised the resulting need for risk-adequate regulation in order to promote innovation and growth on the one hand and to minimise the potential for abuse and systemic risks on the other.[1478] The aim of this chapter is therefore to shed light on the regulatory framework for data-based business models in the digital economy and to highlight the associated legal difficulties and challenges.

1473 Drewes/Meyer/Moss, RDi 2024, 310
1474 See also the comments under B. II. 3. d); in more detail *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 49; *Wagner/Eidenmüller*, ZfPW 2019, 220, 245.
1475 *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 53 et seq.
1476 *Lennartz*, *NJW* 2023, 3543.
1477 *Paal/Hüger*, MMR 2024, 540, 542.
1478 COM(2020) 66 final.

A. Product-related regulation

Bibliography

Ehring, P., & Taeger, J. (eds.), Produkthaftungs- und Produktsicherheitsrecht – Kommentar, 1st ed., Nomos 2022; European Commission, Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final; European Commission, Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final; Hornung, G., & Schallbruch, M. (eds.), IT-Sicherheitsrecht – Praxishandbuch, 2nd ed., Nomos 2024; Kapoor, A., & Klindt, T., ",New Legislative Framework' im EU-Produktsicherheitsrecht – Neue Marktüberwachung in Europa?" *EuZW* (2008), 649; Kirchner, R., Heger, A., Hofmann, R., & Kadelbach, S. (eds.), Digitalisierung im Recht der EU, Nomos 2023; Krönke, C., "Das europäische KI-Gesetz: Eine Verordnung mit Licht und Schatten," *NVwZ* (2024), 529; Martini, M., & Wendehorst, C. (eds.), KI-VO – Verordnung über künstliche Intelligenz, Kommentar, 1st ed., C.H. Beck 2024; Pilniok, A., "Unionsrechtliche Regulierung des Einsatzes von KI-Systemen in der öffentlichen Verwaltung," *DÖV* (2024), 581; Schucht, C., "Die neue Architektur im europäischen Produktsicherheitsrecht nach New Legislative Framework und Alignment Package," *EuZW* (2014), 848; Schwartmann, R., Keber, T., & Zenner, K. (eds.), KI-VO – Leitfaden für die Praxis, 1st ed., C.F. Müller 2024; Voigt, P., & Hullen, N. (eds.), Handbuch KI-Verordnung – FAQ zum EU AI Act, Springer 2024; Wegener, B., Europäische Querschnittpolitiken – Enzyklopädie Europarecht, Band 8, 2nd ed., Nomos 2021.

Advancing digitalisation and the growing use of **data-based business models** pose new regulatory challenges for the European economy. In this context, **product-related regulation** plays a central role in ensuring cybersecurity and the resilience of digital infrastructures. Product-related regulation is characterised by the fact that legal standards are always linked to the characteristics and properties of the product that the legislator considers to be in need of regulation.[1479] Typical regulatory instruments here are regularly security standards or certification obligations for the respective product.[1480]

In contrast**, function-based regulation**[1481] addresses the use or operation of a specific technology or service, regardless of its physical state or specific product characteristics. The legislator specifies requirements for the way in which a particular service may be provided, for example by requiring providers of such services to fulfil certain duties of care when providing the service.[1482]

1479 On the regulatory approach of European product safety law based on the New Legislative Framework, Decision 768/2008/EC of 9 July 2008, Regulation (EC) No. 765/2008 of 9 July 2008 and Regulation (EU) No. 2019/1020 of 20 June 2019.

1480 See, for example, the individual acts on specific product types, e.g. for construction products (Regulation (EU) No. 305/2011), medical devices (Regulation (EU) No. 2017/745) and machinery (Regulation (EU) No. 2023/1230).

1481 See under B.

1482 For example, the provisions of Regulation (EU) 2022/1925, Regulation (EU) 2022/2065, Regulation (EU) 2019/1150.

With the increasing integration of IT systems and data-intensive applications, the threat of cyberattacks, security breaches and operational disruptions has increased significantly. This development has prompted the European legislator to introduce a comprehensive legislative package of measures to strengthen cyber security and operational resilience.[1483] According to the view expressed here, the term **cyber security** refers to protective measures aimed at making unauthorised access to information technology systems as difficult as possible for attackers, regardless of the type of systems or the motives of the attackers.[1484] The legislative package of measures, which can be summarised as **European cybersecurity law,** includes the **NIS 2 Directive**[1485] , the **Cybersecurity Act**[1486] (CSA), the **Cyber Resilience Act**[1487] (CRA) and the **Digital Operational Resilience Act**[1488] (DORA).[1489] These legal acts aim to define technical requirements for products and services in the digital space as well as to strengthen the security of the digital infrastructure as a whole.[1490] While the NIS 2 Directive expands and specifies the cybersecurity requirements for essential and important facilities in the European Union, the CRA explicitly addresses product security in the context of products with digital elements and sets requirements for the security of networked products throughout their entire life cycle.[1491] To further this, the Cybersecurity Act establishes an EU-wide harmonised certification system for products, processes and services in the area of cybersecurity.[1492] Finally, with DORA, the EU legislator has created specific regulations for the strategically important financial sector in order to strengthen its resilience to IT-based risks while paying respect to its unique challenges.[1493]

The product-related regulatory approach also comes into play in the context of **European Artificial Intelligence Act (AIA)**.[1494] The regulation on artificial intelligence[1495] is characterised by the guiding

1483 JOIN(2017) 450 final; Kipker, D./Fischer, M., Cybersecurity-Handbuch, Chapter 21.1 para. 1.

1484 Kirchner, R./Heger, A./Hofmann, R./Kadelbach, S./Roth-Isigkeit, D., Digitalisierung im Recht der EU, p. 230.

1485 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148, OJ L 333, 27 December 2022, pp. 80-152.

1486 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology cybersecurity certification and repealing Regulation (EU) No 526/2013, OJ L 151, 7 June 2019, pp. 15-69.

1487 Regulation (EU) 2024/XX of the European Parliament and of the Council of XX on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, OJ L XX, XX 2024.

1488 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience in the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333, 27.12.2022, p. 1-79.

1489 It should be noted that this includes a large number of other regulations and directives and the list is not exhaustive. For capacity reasons, only the legal acts listed here will be analysed in more detail.

1490 JOIN(2020) 18 final.

1491 Rec. 3, 24 CRA-D.

1492 Hornung, G./Schallbruch, M./Gitter, R., IT-Sicherheitsrecht, sec. 15 para. 26.

1493 Rec. 3 Regulation (EU) 2022/2554.

1494 See Schwartmann, R./Keber, T./Zenner, K./Köhler, M., KI-VO, Part 2 Chapter 1 para. 45; Krönke, C., *NVwZ* 2024, 529 (530) et seq.; Pilniok, A., *DÖV* 2024, 581 (584).

1495 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013,

principle that the requirements and obligations regarding certain AI systems relate primarily to the development of safe systems and not to their use.[1496] The prerequisite is therefore always the existence of a previously defined AI system.[1497] Its character as a 'product safety law' is particularly evident in the provisions on high-risk AI systems: For such systems, the AIA provides, for example, for the establishment of a special risk management system (Art. 9 AIA), requirements for the handling of training, validation and test data (Art. 10 AIA), documentation of the systems (Art. 11 AIA) and automatic logging of events during the entire life cycle of the AI systems (Art. 12 AIA). However, the EU legislator sometimes meanders between its regulatory concepts, as some provisions of the AIA make clear. In particular, the provisions prohibiting certain practices in the field of AI (Art. 5 AIA) and the provider obligations of Art. 55(1) AIA primarily address the risks of using certain AI systems.[1498]

At its core, however, the AIA is based on the product-related regulatory concept that finds its origins in the **New Legislative Framework**[1499]. This Framework, in turn, is founded on the European harmonisation concept of the **New Approach** that emerged during the 1980s.[1500] This regulatory approach, which stands in contrast to the function-based regulation of platforms, online marketplaces and gatekeepers, is also the guiding principle of European product safety law.[1501]

(EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, OJ L, 2024/1689, 12.7.2024.

1496 Krönke, C., *NVwZ* 2024, 529 (530) et seq.

1497 Martini, M./Wendehorst, C., KI-VO, Art. 1 para. 7 also speak of a technology-related approach in this respect.

1498 Krönke, C., *NVwZ* 2024, 529 (531), (533) et seq.

1499 https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en?prefLang=de (last accessed on: 1 November 2024).

1500 See also Voigt, P./Hullen, N., Handbuch KI-Verordnung, Chapter 1.1; in detail on the New Legislative Framework Schucht, C., *EuZW* 2014, 848; Kapoor, A./Klindt, T., *EuZW* 2008, 649.

1501 Ehring, P/Taeger, J./Heuser, J., Produkthaftungs- und Produktsicherheitsrecht, Vorbem. §§ 99 ff ProdSG para. 2, 3; on technology law see also Wegener, B./Führ, M., Europäische Querschnittpolitiken, § 4 para. 109, 120.

I. European cyber security law

1. Network and Information Security Directive (NIS) - Directive (EU) 2022/2555

Bibliography

German Federal Ministry of the Interior and for Home Affairs, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (cited as: BMI, NIS 2-Referentenentwurf, p.); Hajek Gross, C., & Wünnerke, F., "Fahrtrichtung Zukunft: NIS 2-Richtlinie und ihre Auswirkungen auf die Automobilindustrie," *RAW* (2024), 117; Hessel, S., Callewaert, C., & Schneider, M., "Die NIS-2-Richtlinie aus Unternehmensperspektive," *RDi* (2024), 208; Hessel, S., Callewaert, C., & Schneider, M., "Firewalls und Familiengeschäfte: Das neue Cybersicherheitsrecht für den Mittelstand," *RFamU* (2024), 200; Leßner, A., "Konzernspezifische Änderungen aus der NIS 2-Richtlinie und ihre Umsetzung," *MMR* (2024), 226; Leßner, A., & Mayr, L., "Besonderheiten für Konzerne in den NIS-Richtlinien und dem BSIG," *MMR* (2024), 148; Kipker, D. (ed.), Cybersecurity-Handbuch, 2nd ed., C.H. Beck 2023; Kipker, D., Birreck, P., Niewöhner, M., & Schnorr, T., "NIS-Richtlinie und der Entwurf der NIS-2-Richtlinie," *MMR* (2021), 214; Vettermann, O., "Geordnetes Chaos in der Sicherheitsforschung?" *MMR* (2023), 827; Voigt, P., & Bastians, H., "Neue europarechtliche Anforderungen an die IT-Sicherheit Rat der EU nimmt NIS 2-Richtlinie an – ein erster Überblick," *CR* (2022), 768.

a) Introduction

The Directive on measures for a high common level of cybersecurity across the Union (NIS 2)[1502] was published in the Official Journal of the EU on 27 December 2022 and entered into force on 16 January 2023. The NIS 2 Directive is the direct successor to the NIS Directive, which aimed to build cybersecurity capabilities across the EU.[1503] The aim was to mitigate existing threats to network and information systems that provide essential services. The measures were intended to enable an adequate response to security incidents and to ensure the continuity of essential information and communication services.[1504]

Although considerable progress has been made in the area of cyber resilience within the European Union since the NIS Directive came into force, the previous directive also had significant shortcomings that impaired its effectiveness in terms of current and future cyber resilience challenges.[1505] As it is a directive in legal terms that requires implementation in the member states by means of national transposition laws, implementation in the member states has varied greatly, which runs counter to the goal of strengthening cyber resilience across the EU.[1506]

1502 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, OJ L 333, 27.12.2022, p. 80-152.

1503 Rec. 1 Directive (EU) 2022/2555.

1504 Rec. 1 Directive (EU) 2022/2555.

1505 Rec. 2 Directive (EU) 2022/2555.

1506 Kipker, D./Fischer, M., Cybersecurity-Handbuch, Chapter 21 para. 5; Voigt, P./Bastians, H., *CR* 2022, 768 (769).

The NIS 2 Directive lays down measures to ensure a high common level of cybersecurity throughout the Union in order to ensure and improve the functioning of the internal market, Art. 1(1) Directive (EU) 2022/2555.[1507]

The directive is to be implemented by 18 October 2024, and must consequently, it must be incorporated into national law by the member states by this date.

b) Scope, Art. 2 Directive (EU) 2022/2555

The NIS 2 Directive applies to all **public** and **private organisations** of the type listed in Annex I and II that are considered medium-sized enterprises in accordance with Art. 2 Annex to Recommendation 2003/361/EC or that exceed the thresholds for medium-sized enterprises and provide their services in the Union or carry out their activities there, Art. 2(1) Directive (EU) 2022/2555.

aa) Establishment, Art. 6 No. 38 Directive (EU) 2022/2555

According to Art. 6 No. 38 Directive (EU) 2022/2555, an organisation is a natural or legal person that can exercise rights and be subject to obligations in its own name. A medium-sized company is defined as having between 50 and 250 employees, a turnover of EUR 10–50 million and an annual balance sheet total of no more than EUR 43 million. Companies that exceed these thresholds are also covered by the NIS 2 Directive.[1508]

Annexes I and II of the NIS 2 Directive contain a detailed list of the facilities covered, differentiated by sector, sub-sector and type of facility. The sectors of **high criticality** listed in **Annex I** include energy (No. 1), transport (No. 2), banking (No. 3), financial market supervision (No. 4), healthcare (No. 5), drinking water (No. 6), waste water (No. 7), digital infrastructure (No. 8), ICT service management (No. 9), public administration (No. 10) and space (No. 11); **Annex II**, on the other hand, lists **other critical sectors**, which include postal and courier services (No. 1), waste management (No. 2), production, manufacture and trade of chemicals (No. 3), production, processing and distribution of food (No. 4), manufacturing/production of goods (No. 5) and digital service providers (No. 6). Within the energy sector and the hydrogen sub-sector, for example, operators in the field of hydrogen production, storage and transmission are included.

bb) Facilities covered regardless of their size, Art. 2(2) Directive (EU) 2022/2555

Article 2(2) of the NIS 2 Directive also mentions a number of other companies that fall within the scope of the Directive, regardless of their size. Particularly vulnerable or important organisations with a high interest in the continuity of the services they provide are included here.[1509] The provisions therefore apply, among others, to providers of public electronic communications networks or publicly available electronic communications services (Art. 2(2)(a)(i) Directive (EU) 2022/2555) and also to organisations

---

1507 Kipker, D./Fischer, M., Cybersecurity-Handbuch, Chapter 21 para. 4.

1508 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC), OJ 2003 L 124, 36.

1509 Kipker, D./Birreck, P./Niewöhner, M./Schnorr, T., *MMR* 2021, 214 et seq.

in which a disruption of the service they provide could have a significant impact on public order, public security or public health (Art. 2(2)(c) Directive (EU) 2022/2555).

Regulated are also, regardless of the size of the facility, critical facilities under the CER Directive[1510] that provide domain registration services, Art. 2(3), (4) Directive (EU) 2022/2555.

cc) Essential and important facilities, Art. 3 (1), (2) Directive (EU) 2022/2555

A distinction is made between two categories of facilities that fall under the scope of the NIS 2 Directive: **Essential and important institutions**, Art. 3 (1), (2) Directive (EU) 2022/2555. The distinction is made on the basis of their criticality in relation to their sector or the type of services they provide and their size.[1511]

c) Obligations of covered entities, Art. 20 et seq. Directive (EU) 2022/2555

The main obligations for the organisations covered by the NIS 2 Directive are set out in Chapter IV of the Directive, in Art. 20 et seq. Directive (EU) 2022/2555.

aa) Risk management measures in the area of cybersecurity, Art. 21 Directive (EU) 2022/2555

According to Article 21(1) Directive (EU) 2022/2555; organisations must therefore take appropriate and proportionate measures to manage the risks to the security of the network and information systems they use for the operation or provision of their services and to prevent or minimise the impact of security incidents on the recipients of their services and on other services. It follows from the wording, "[...] *based on a security-neutral approach aimed at* [...]", of Article 21(2) Directive (EU) 2022/2555 that the Directive requires neither absolute security nor the highest possible level of security. Rather, the facilities must guarantee a level of safety depending on the existing risk.[1512]

The German legislator has already implemented a corresponding regulation in Section 30(1) BSIG and – over and above the requirements of the directive – has provided for a documentation obligation, according to which the organisations are obliged to adequately document the implementation of and compliance with the measures.[1513]

Most of the minimum measures listed in Art. 21(2) Directive (EU) 2022/2555 and Section 30(2) BSIG are likely to have already been implemented by the affected companies, as they are part of the standard

---

1510 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (EU) 2022/2557, OJ L 333, 27.12.2022, p. 164-198.

1511 Rec. 15 Directive (EU) 2022/2555, OJ L 333/80; Kipker, D./Fischer, M., Cybersecurity-Handbuch, Chapter 21.1 para. 6.

1512 Hessel, S./Callewaert, C./Schneider, M., *RDi* 2024, 208 (212).

1513 BMI, NIS 2 Draft, p. 160.

repertoire of internal cyber resilience. These include maintaining operations through **backup management** ((c) No. 3), **multi-factor authentication** ((j) No. 10) or the **use of encryption methods** ((h) No. 8).

In accordance with Art. 21(2)(d) Directive (EU) 2022/2555[1514], Section 30(2) No. 4 BSIG, organisations must now also take measures to ensure cyber resilience at their suppliers and service providers, as this is the only way to consistently achieve comprehensive cyber resilience. This means that individual organisation must no longer only take care of its own security concerns, but must also include the potential threats from connections with other organisations in its security concept.[1515] This is because while an organisation may have cyber security measures in place, these are useless if they are reliant on third-party services or products that are not required to take any security measures.[1516] The extension of the obligations to the supply chain could mean that companies that are not actually covered by the NIS 2 Directive are also indirectly regulated.[1517]

bb) Reporting obligations, Art. 23 Directive (EU) 2022/2555

According to Art. 23(1) Directive (EU) 2022/2555, Member States shall ensure that essential and important organisations notify their CSIRT (Computer Security Incident Response Team, which must be set up by the Member States according to Art. 10(1) Directive (EU) 2022/2555) or, where applicable, their competent authorities without undue delay of any security incident that has a significant impact on the provision of their services.[1518]

According to Art. 6 No. 6 Directive (EU) 2022/2555, a security incident is any event that affects the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the services offered or accessible via network and information systems. According to Art. 23(3) Directive (EU) 2022/2555, such a security incident is significant if it has caused or may cause serious disruption to the operation of the services or financial losses for the affected organisation (a). In addition, a significant security incident may also exist if other natural or legal persons are or may be affected by significant material or immaterial damage (b).[1519]

The reporting obligation incumbent on the affected organisation can be divided into a three-stage reporting mechanism consisting of an early warning, an interim report and a final report.[1520] According to Article 23(4)(a) of the NIS 2 Directive, organisations affected by a significant security incident are initially obliged to submit an early warning to the CSIRT or the competent authority immediately, and in any case within 24 hours of becoming aware of the incident, stating whether the significant security

1514 Section 30(2) sentence 2 No. 4 BSIG is relevant for German law.
1515 Hessel, S./Callewaert, C./Schneider, M., *RFamU* 2024, 200 (202).
1516 Hessel, S./Callewaert, C./Schneider, M., *RDi* 2024, 208 (212) et seq.
1517 Hessel, S./Callewaert, C./Schneider, M., *RFamU* 2024, 200 (202).
1518 Voigt, P./Bastians, H., *CR* 2022, 768 (771).
1519 Rec. 101 Directive (EU) 2022/2555.
1520 Hajek Gross, C./Wünnerke, F., *RAW* 2024, 117 (122).

incident is suspected to be the result of unlawful or malicious acts or whether it could have cross-border implications.[1521] In accordance with Art. 24(4)(b) Directive (EU) 2022/2555, a further notification must also be submitted without delay, but in any case within 72 hours (trust service providers only have 24 hours here, Art. 23(4) Directive (EU) 2022/2555), which contains an update of the information transmitted in accordance with Art. 24(4)(a) Directive (EU) 2022/2555 and an initial assessment of the significant security incident. Following this, affected organisations must submit an interim report on any relevant status updates at the request of a CSIRT or a competent authority, Art. 24(4)(c) Directive (EU) 2022/2555. Finally, the organisation must submit a comprehensive final report no later than one month after the notification of the security incident in accordance with Art. 24(4)(b), (d) Directive (EU) 2022/2555.[1522] However, if the security incident is still ongoing at this time, the organisation must submit a progress report at this time and a final report within one month of dealing with the security incident, Art. 24(4)(e) Directive (EU) 2022/2555.

The German national implementation of the reporting obligations of the NIS 2 Directive is primarily set out in Section 32 of the BSIG.

The reports are primarily to be directed to the CSIRTs or the competent authority. However, if the provision of the respective service is affected by the significant security incident, the recipients of the services may also have to be notified, Art. 24(1) Directive (EU) 2022/2555. Such a reporting obligation (regarding all measures, remedial measures or, if applicable, the threat itself) may also apply to the recipients of the services if they could potentially be affected by a significant cyber threat.[1523] Finally, in cases where it is necessary to raise public awareness in order to prevent a significant security incident, to manage a significant security incident that is already underway or where there is another public interest affected, the CSIRT or the competent authority may request the organisation concerned to inform the public, Art. 24(7) Directive (EU) 2022/2555. The public can also be informed by the CSIRT or the competent authority itself.

According to Art. 30(1) Directive (EU) 2022/2555 in addition to the mandatory reporting obligations, the Member States must also ensure that organisations that do not fall within the scope of the NIS 2 Directive, but fit the definition of essential and important organisations, are able to voluntarily report cyber threats, incidents that do not qualify as significant incidents according to Art. 23(3) Directive (EU) 2022/2555 or near-incidents. Organisations not subject to the NIS 2 Directive can also voluntarily report significant security incidents.[1524]

1521 Rec. 102 Directive (EU) 2022/2555.
1522 Rec. 102 Directive (EU) 2022/2555.
1523 Rec. 103 Directive (EU) 2022/2555, Voigt, P./Bastians, H., *CR* 2022, 768 (772).
1524 Rec. 58, 105 Directive (EU) 2022/2555.

cc) Utilisation of the European schemes for cybersecurity certification, Art. 24 Directive (EU) 2022/2555

According to Art. 24(1) Directive (EU) 2022/2555, Member States may require essential and important organisations to use specific ICT products, services and processes that are certified under European cybersecurity certification schemes in accordance with the CSA in order to demonstrate compliance with the requirements of Art. 21. The European Commission can also use implementing acts to determine which categories of essential and important organisations are obliged to use these ICT products, services and processes, Art. 24(2) Directive (EU) 2022/2555. However, these implementing acts are only to be adopted if an inadequate level of cybersecurity has been established, Art. 24(2) Directive (EU) 2022/2555.

d) Supervision, enforcement and sanctions, Art. 31–37 Directive (EU) 2022/2555

With NIS 2 being a directive, the Member States are required to create competence for their national authorities in order to ensure an effective, proportionate and dissuasive sanctions system (Art. 31 et seq. Directive (EU) 2022/2555). The Directive does, however, set out some minimum requirements in this regard in Articles 32, 34 and 35 of the Directive (EU) 2022/2555.

Article 32(4) Directive (EU) 2022/2555 stipulates that the Member States must be given the following minimum powers to enforce the Directive.

The supervisory authorities must be able to issue warnings about breaches by the entities concerned, issue binding instructions and set deadlines for their implementation and issue orders to remedy any deficiencies or breaches identified or to cease the offending behaviour. They must also have the authority to instruct the organisations concerned to inform their users of potential cybersecurity threats and the defensive measures to be taken. They must also be authorised to designate, for a specified period of time, a monitoring officer entrusted with clearly defined tasks to monitor compliance with Articles 21 and 23 by the entities concerned and to instruct the entities concerned to publicly disclose aspects of breaches of this Directive in accordance with specified requirements.

According to Article 32(7) of the NIS 2 Directive, the competent authorities must respect the rights of the defence and take into account the circumstances of the individual case when taking enforcement measures and imposing sanctions.[1525] The authorities take into account, for example, the severity and duration of the attempts, the damage caused, any intent or the extent of cooperation with the authority in the assessment and, depending on this, determine the amount of the fine and the respective measure, Art. 32(7)(a) – (h) Directive (EU) 2022/2555.

The fines are issued in addition to the measures set out in Art. 42(4) Directive (EU) 2022/2555 and the same considerations as in Art. 32(7) Directive (EU) 2022/2555 must be included in the assessment when

[1525] Rec. 133 Directive (EU) 2022/2555.

determining the amount, Art. 34(2), (3) Directive (EU) 2022/2555. For breaches of Art. 21 and 23 Directive (EU) 2022/2555, the organisation must pay a specific fine in accordance with Art. 34(4), (5) Directive (EU) 2022/2555, depending on whether it is an important or essential organisation. Important institutions pay a maximum amount of at least EUR 7 million or 1.4 % of the previous year's turnover, whichever is higher. Essential entities pay EUR 10 million or 2 % of the previous year's turnover, whichever is higher.

The risk of fines is likely to increase for groups with the implementation of the NIS 2 Directive because, according to the ECJ's understanding of the term[1526], the "functional concept of an undertaking" includes all group companies and the calculation of the previous year's turnover could therefore be aggregated from the turnover of the entire group.[1527]

If a breach of Art. 21 or 23 Directive (EU) 2022/2555 also constitutes a reportable personal data breach within the meaning of Art. 33 GDPR, the supervisory authority must immediately notify the supervisory authorities referred to in Art. 55 or 56 GDPR in accordance with Art. 35 (1) Directive (EU) 2022/2555.

e) Summary and practical implications

The NIS 2 Directive expands the scope to include more companies and sectors such as public administration, postal and courier services, waste management and food production and processing, which requires cybersecurity measures to be adapted or reorganised. Companies must implement stricter requirements for risk management and reporting obligations in order to avoid higher liability and sanction risks. There is a greater onus on company management to provide cybersecurity resources, while cross-border activities require harmonised implementation. Companies must also ensure that their service providers and partners fulfil the new security requirements. In practice, however, these requirements lead to uncertainties with regard to specific measures within the company.

The German legislator's previous draft legislation (NIS 2UmsuCG) does not fulfil the expectations of a comprehensive adaptation of the BSIG, as there are still uncertainties regarding the inclusion of cross-sectional tasks and cross-sector activities.[1528]

The fourth draft bill published by the Federal Ministry of the Interior on 26 June 2024[1529] continues to be widely criticised. The main criticism is that the NIS 2 Directive cannot guarantee a high common level of cybersecurity, as administrations at municipal and state level are exempt from the obligations of the directive in the German transposition law. However, it is precisely these authorities that have

1526 ECJ, judgement of 23 April 1991 - C-41/90 para. 21; ECJ, decision of 12 July 1984 – C-170/83 para. 11.
1527 Leßner, A./Mayr *L.*, *MMR* 2024, 148 (152).
1528 Vettermann O., *MMR* 2023, 827 (831).
1529 Draft law to implement the NIS 2 Directive and to regulate the essential principles of information security management in the federal administration, available at https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenen-wuerfe/CI1/NIS-2-RefE-24062024.html (last accessed on: 1 November 2024).

increasingly fallen victim to cyber attacks in the past.[1530] The current draft law does contain some clarifications for affected organisations that are also subject to regulation by other legal acts due to their sectoral affiliation, which are certainly welcomed by practitioners.[1531] Furthermore, the draft law has been the subject of criticism on the grounds that it is excessively vague with regard to the measures to be taken by the operators. This has resulted in a situation in which operators are unable to recognise which additional measures they are now obliged to take. In particular, it should be noted here that, according to the government draft, only those parts of the organisation that fall within one of the regulated sectors are to be taken into account as part of the impact analysis. Cross-sector activities such as personnel management are only to be taken into account on a pro rata basis. However, it is not clear to what extent cross-divisional tasks are to be included and which activities are covered at all. Finally, it is not foreseeable whether this restriction of the scope can be maintained, as a comparable limitation is not provided for in the NIS 2 Directive.[1532] For many companies that are active in the ICT sector and belong to a group of companies, the applicability of the NIS 2 Directive and the new BSIG will have to be redefined in accordance with these rules.[1533] Medium-sized and family-owned companies will also have to face the sometimes complex and sprawling scope regulations.[1534] Whether and when changes can be expected with regard to the criticisms levelled at the planned 'NIS 2 Umsetzungsgesetz' now depends largely on the parliamentary deliberations in the Bundestag and Bundesrat, which must now debate and pass the law following the cabinet's decision. The requirements could also be fine-tuned by means of more specific legal ordinances. While other member states such as Belgium have already transposed the requirements of the directive into national law on time, the 'NIS 2 Umsetzungsgesetz' is not expected to come into force until spring 2025.[1535]

1530 Interview NJW/Stephan Schmidt "Eine absolute Sicherhiet gibt es nicht mehr ", available at https://rsw.beck.de/aktuell/daily/magazin/detail/interview-*NJW*-2024-33-eine-absolute-sicherheit-gibt-es-nicht-mehr (last accessed on: 1 November 2024).

1531 NIS 2 Directive: New draft implementing acts published, available at https://www.noerr.com/de/insights/NIS 2-richtlinie-neue-entwurfe-von-umsetzungsrechtsakten-veroffentlicht (last accessed on 1 November 2024).

1532 NIS 2 Implementation Act - Need for action for affected companies despite many unanswered questions, available at https://www.roedl.de/themen/NIS 2-umsetzungsgesetz-handlungsbedarf-betroffenheit-offene-fragen (last accessed on: 1 November 2024).

1533 Leßner *A.*, *MMR* 2024, 226 (228).

1534 Hessel S./Callewaert C./Schneider M., *RFamU* 2024, 200 (201).

1535 On the implementation status in the Member States https://www.openkritis.de/eu/eu-mitgliedsstaaten-nis-2.html (last accessed on: 1 November 2024).

2. Cybersecurity Act (CSA) - Regulation (EU) 2019/881 (overview)

Bibliography

Hornung, G., & Schallbruch, M. (eds.), IT-Sicherheitsrecht – Praxishandbuch, 2nd ed., Nomos 2024; Kipker, D., Reusch, P. & Ritter, S. (eds.), Recht der Informationssicherheit, 1st ed., C.H. Beck 2023; Kipker, D. (ed.), Cybersecurity-Handbuch, 2nd ed., C.H. Beck 2023.

The Cybersecurity Act (CSA)[1536] was published in the Official Journal of the European Union on 7 June 2019 and came into force twenty days later. All provisions of the regulation would apply from 28 June 2021. This regulatory act essentially establishes two aspects of the European cybersecurity concept:

Firstly, the CSA introduces the **European Union Agency for Cybersecurity (ENISA).**[1537] The acronym 'ENISA' – as well as all decisions, agreements and property, Art. 68 CSA – remain from the old agency, which was established in 2004 by Regulation (EC) 460/2004[1538] as a non-permanent European Network and Information Security Agency.[1539] Articles 2 to 45 CSA regulate the objectives, the official structure, the working methods, the budget and the staff of the organisation. In contrast to its predecessor organisation, the international authority has a permanent mandate and more extensive powers, responsibilities and resources.[1540] ENISA has a wide range of tasks, but there are essentially four main areas of responsibility.[1541] (1) ENISA directly supports the European legislator in legislation and regulatory strategy. (2) ENISA maintains close contact with the national authorities (in particular CSIRTs) and thus organises cross-border operational cooperation. (3) ENISA builds up human and technical capacities, for example by providing information material and organising expert forums. (4) ENISA issues cybersecurity certificates for digital products and services.

Secondly, the CSA establishes a standardised framework for the definition of European schemes for the cybersecurity certification of **information and communication technology** (ICT) products.[1542] Articles 46 to 65 of the CSA regulate the certification system and the respective requirements for certification bodies. In principle, the CSA is based on voluntary certification by an economic operator in its own interest, although mandatory certificates are also reserved in certain areas, Art. 56(2) CSA.[1543] ENISA

1536 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communication Technology cybersecurity certification, OJ 151/15.

1537 For further information on the agency, see Kipker, D./Fischer, M., Cybersecurity-Handbuch, Chap. 21.1 para. 2 et seq.

1538 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

1539 Kipker D./Reusch P./Ritter S./Wenning R., Recht der Informationssicherheit, Art. 1 CSA para. 10 et seq.

1540 Hornung, G./Schallbruch, M./Gitter, R., IT-Sicherheitsrecht, Section 15 para. 26.

1541 https://www.enisa.europa.eu (last accessed on: 1 November 2024).

1542 Kipker, D./Fischer, M., Cybersecurity Handbook, Chapter 21.1 para. 17.

1543 Hornung, G./Schallbruch, M./Gitter, R., IT-Sicherheitsrecht, Section 15 para. 26; Kipker, D./Fischer, M., Cybersecurity-Handbuch, Chapter 21.1 para. 18.

is developing a scheme for cybersecurity certification on behalf of the Commission, Art. 48 et seq. CSA. ENISA maintains a website[1544], which contains information on all developed schemes, certifications and declarations of conformity, Art. 50 CSA. Depending on the security requirements, the certification schemes indicate the trustworthiness in one of three levels. The **ICT product** can therefore be categorised into the assurance levels "basic", "substantial" and "high", Art. 52(1), (5), (6), (7) CSA. The "substantial" level assumes that the certified ICT product can withstand cyberattacks by actors with limited resources; "high" proves that the product is also immune to attacks by actors with extensive resources, Art. 52(5) et seq. CSA.

The cyber security certification schemes are used in the draft 'Cyber Resilience Act'[1545] , among others. There, the manufacturer has the option of providing the proof of conformity of its products with the technical specifications by means of a certificate with at least the "substantial" assurance level.

[1544] https://www.enisa.europa.eu/ (last accessed on: 1 November 2024).

[1545] Position of the European Parliament adopted at first reading on 12 March 2024; available at https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_DE.html (last accessed on: 1.11.2024).

3. Cyber Resilience Act (CRA) – Regulation (EU) 2024/2847

Bibliography

Biendl, M., & Füllsack, J., "Der finale Cyber Resilience Act im Überblick – Anwendungsbereich, Pflichten und Sanktionen," *CR* (2024), 376; Chiara, F., "The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements," *International Cybersecurity Law Review*, Vol. 3 (2022), 255; Dittrich, T., & Heinelt, C., "Compliance-Pflichten für Hersteller nach dem Cyber Resilience Act," *RDi* (2023), 309; Fellner, F., *Normung für alle – Eine Einführung plus CE für Druckgeräte und Maschinen*, 2nd ed., Springer Vieweg 2023; Heckmann, D., & Ziegler, N., "Der Cyber Resilience Act: Ein Gesetz mit digitalen Elementen," *ITRB* (2024), 159; Hessel, S., & Callewaert, C., "Der Cyber Resilience Act der EU-Kommission," *K&R* (2022), 789; Piltz, C., Weiß, A., & Zwerschke, J., "Der Vorschlag für einen Cyber Resilience Act aus Sicht der DS-GVO – Überblick zum Anwendungsbereich, den rechtlichen Anforderungen und dem Konformitätsverfahren," *CR* (2023), 154; Poncza, M., "Der Entwurf des Cyber Resilience Act," *ZfPC* (2023), 44; Poncza, M., Keppeler, L., & Lennartz, M., "Die Open-Source-Bereichsausnahme im Entwurf des Cyber-Resilience-Act," *ZfPC* (2023), 117; Rennert, J., "Mehr Cybersicherheit für vernetzte Produkte: Der Vorschlag der EU-Kommission für einen ‚Cyber Resilience Act'," *ZfDR* (2023), 206; Roth-Isigkeit, D., "Der risikobasierte Ansatz als Paradigma des Digitalverwaltungsrechts," *MMR* (2024), 621; Ruttloff, M., Wagner, F., & Stilz, M., "Der Entwurf des Cyber Resilience Act und seine Auswirkungen auf das Gewährleistungs- und Produkthaftungsrecht," *BB* (2024), 1603; Siglmüller, J., "Cyber Resilience Act und Digital Operational Resilience Act – Lässt sich IT Sicherheit rechtlich erzwingen?" *ZfPC* (2023), 221; Schweinoch, M., & Meßmer, D., "Vorschlag der EU-Kommission für einen ‚Cyber Resilience Act'," *CR* (2022), R112; Schöttle, H., "Cyber Resilience Act, Produkthaftungsrichtlinie und andere Baustellen für die Open Source Communities," *ZfPC* (2023), 215; Vettermann, O., "Geordnetes Chaos in der Sicherheitsforschung?" *MMR* (2023), 827; Vettermann, O., "Die digitale Identität (EU's Version)," *RDi* (2024), 260; Voigt, P., & Falk, L., "Der Cyber Resilience Act," *MMR* (2023), 88; Wagner, E., Holm-Hadulla, E., & Ruttloff, M. (eds.), Metaverse und Recht, 1st ed., C.H. Beck 2023; Weiden, H., "Aktuelle Berichte – Mai 2024," *GRUR* (2024), 669; Wiebe, G., "Cybersicherheitsrecht 2.0 – Vorschlag eines Cyber Resilience Act," *ZRP* (2023), 73; Wiebe, G., & Daelen, J., "Der Cyber Resilience Act aus produktsicherheitsrechtlicher Perspektive," *EuZW* (2023), 257; Zirnstein, Y., "Better Cybersecurity due to increased regulation? The final European Cyber Resilience Act," *Cri* (2024), 65; Zirnstein, Y., "Der Entwurf des Cyber Resilience Act," *CR* (2022), 707.

a) Introduction

On 15 September 2022, the European Commission published its proposal for a regulation on horizontal cybersecurity requirements for products with digital elements, the Cyber Resilience Act. On 12 March 2024, the amended draft of the CRA was then adopted at first reading by the European Parliament's Committee on Industry, Research and Energy. On 10 October 2024, the Council of the European Union

adopted the Cyber Resilience Act (CRA).[1546] On 20 November 2024, the Cyber Resilience Act was published in the Official Journal of the European Union.[1547]

With the CRA, a binding and, in particular, horizontal, i.e. cross-sectoral, regulatory act is to be created for the first time across the EU, which provides for minimum requirements for the cybersecurity of digital products.[1548] As part of the European Union's comprehensive digital strategy, the CRA serves as a supplement to the NIS 2 Directive[1549] for the area of IT product security.[1550] It is categorised under product safety law and uses familiar building blocks and regulatory techniques from the 'New Legislative Framework'[1551] (NLF).[1552]

The CRA has two main regulatory objectives under the framework objective of a properly functioning internal market: Firstly, to create the legal basis for the development of secure products with digital elements so that they are placed on the market with fewer vulnerabilities and so that the manufacturer maintains technical support with regard to cybersecurity for the entire "lifetime" of the product.[1553] On the other hand, conditions should also be created for the users of digital products that enable them to consider cybersecurity as a decisive selection and usage criterion with regard to the digital product.[1554]

One of the ways in which these objectives are to be achieved is by requiring manufacturers to consider the security of the products they develop with digital elements from the development phase onwards and to maintain and improve this security throughout the entire life cycle of the product.[1555] Furthermore, the CRA is intended to create a standardised **cybersecurity framework** for hardware and software products for the first time, which should make it much easier for manufacturers to comply with the regulations.[1556] Finally, regulatory instruments such as cybersecurity certificates are intended to increase transparency with regard to the security features of products with digital elements. The overall aim is to enable entrepreneurs and consumers to use products with digital elements safely.[1557]

1546 See EU Council press release 752/24 of 10 October 2024, available at: https://www.consilium.europa.eu/de/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/pdf/ (last accessed on: 1 November 2024).

1547 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 20.11.2024 p. 1/81.

1548 Rec. 4 CRA.

1549 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union

1550 Vettermann, O., *RDi* 2024, 260 (266); Vettermann, O., *MMR* 2023, 827 (830).

1551 New legislative framework, available at: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework (last accessed on: 1 November 2024).

1552 Wiebe, G./Daelen, J., *EuZW* 2023, 257.

1553 Rec. 2 p. 1 CRA.

1554 Rec. 2 p. 2 CRA.

1555 Art. 13 et seq. CRA; Rec. 10 et seq. CRA.

1556 Rec. 4 CRA.

1557 COM(2022) 454 final, p. 1 et seq.

b) Interaction with other legal acts

The CRA contains explicit exemptions for certain products that are already covered by more specialised EU legislation. To this end, the CRA defines a basic conflict-of-law rule for more specialised EU legislation, namely that the scope of the CRA remains excluded if the sector-specific regulation achieves the same or a higher level of protection than the CRA and a committee would not be incompatible with the general legal framework, Art. 2(5) CRA – the CRA thus guarantees a minimum standard of product cybersecurity.[1558] Overlaps may arise in particular with general IT product security provisions of the NIS 2 Directive, the GDPR, the AIA and other EU product security legislation.

aa) NIS 2-RL

With regard to the NIS 2 Directive, which sets out IT security requirements for the protection of critical infrastructures, the CRA can be seen as a supplement to the Directive, as some of the organisations affected cannot effectively influence many of the existing cyber security risk potentials.[1559] The CRA therefore places a direct obligation on manufacturers of products with digital elements to create a secure and resilient ecosystem using resilient digital products. For example, ICT service providers can take risk management measures for the security and risks of their own ICT network in accordance with Art. 21(1) Directive (EU) 2022/2555, but not for the many end devices that access their services and potentially add further security vulnerabilities to the system.

bb) CSA

The CSA continues ENISA as an international authority, Art. 3–45 CSA, and introduces a European system for cybersecurity certification, Art. 46–65 CSA. The CRA utilises these infrastructures, for example in Art. 32 CRA, and thus fits into existing cybersecurity law.

cc) GDPR

Overlaps with the GDPR may arise in particular in connection with data protection certification procedures, data protection seals and certification marks, Art. 42 GDPR.[1560] According to the legislator's ideas, such mechanisms can be implemented in products with digital elements, thereby creating synergy effects. This further demonstrates the standard setter's complementary understanding of cybersecurity and the protection of personal data.[1561] Otherwise, the applicability of the GDPR remains unaffected.

dd) Product Safety Regulation

Other EU product safety legislation is generally applicable in addition to the CRA, unless corresponding regulations are expressly excluded.[1562] This applies in particular to the Product Safety Regulation[1563],

---

1558 Rec. 28 CRA; Wiebe, G./Daelen, J., *EuZW* 2023, 257 (259).
1559 Rec. 3, 24 CRA.
1560 Rec. 32 CRA.
1561 Rec. 32 CRA; Hornung, G./Schallbruch, M., IT-Sicherheitsrecht, Section 1 para. 21 with further references.
1562 Ruttloff, M./Wagner, F./Stilz, M., *BB* 2024, 1603 (1605); Wiebe, G./Daelen, J., *EuZW* 2023, 257 (258).
1563 Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, OJ L 135/1, 23.5.2023, p. 1-51.

which declares Art. 11 CRA to be largely applicable to products with digital elements with regard to safety risks. The legislator thus recognises that products with digital elements also harbour other safety risks that are only indirectly related to the cybersecurity of the product.[1564]

ee) Product Liability Directive

The upcoming new product liability directive[1565] is applicable alongside the CRA. It regulates the manufacturer's strict liability for defective products that cause damage due to cybersecurity defects, among other things.[1566]

ff) Regulation on the European Digital Identity (EUDI)

If products are also covered by the European Digital Identity Regulation[1567] and are certified in accordance with this regulation, the manufacturer can derive a presumption of conformity for the CRA in accordance with Art. 27(1) CRA.[1568]

gg) AIA

The AIA also applies alongside the future CRA.[1569] Overlaps may arise if a product with digital elements is also categorised as a high-risk system in accordance with Art. 6 CIR.[1570] Art. 12 CRA explicitly regulates the conditions under which such a product with digital elements is deemed to be compliant (within the meaning of the CRA) with the requirements set out in Art. 15 AIA. For example, high-risk systems that have undergone a conformity assessment in accordance with the AIA and at the same time constitute important or critical products in accordance with the CRA are to be regarded as compliant with the requirements of the CRA; however, in no case does this reduce the required trustworthiness of a product in accordance with the CRA.[1571]

c) Scope and definition

aa) Material scope: Products with digital elements, Art. 2(1) CRA

According to Art. 2(1) CRA, the Regulation applies to all **products with digital elements** (hereinafter: products) made available on the market that can establish a direct or indirect logical or physical data connection to a device or network. According to Art. 3 No. 1 CRA, products with digital elements are all software or hardware products and their remote data processing solutions, including software or

1564 Rec. 50 CRA.
1565 European Commission, Proposal for a Directive on liability for defective products, 28.9.2022, COM(2022) 495 final.
1566 Rec. 31 CRA.
1567 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, OJ L 257/73, 28.8.2014, p. 73-114.
1568 Rec. 33 CRA.
1569 Heckmann, D./Ziegeler, N., *ITRB* 2024, 159 (160); Zirnstein, Y., *CRi* 2024, 65 (67); Zirnstein, Y., *CR* 2022, 707 (708).
1570 Rec. 51, 14 CRA.
1571 Rec. 51 CRA.

hardware components (Art. 3 No. 4 and 5 CRA), being placed on the market separately. As a sign of the horizontal regulatory approach, the definition of products with digital elements is broad.[1572] According to the recitals, repaired and otherwise modified products are also covered by the scope of the CRA if the product is significantly modified, i.e. in a way that goes beyond the original risk assessment.[1573] Software updates are equivalent to physical changes.[1574] The draft categorises products with digital elements according to a risk-based approach into important products with digital elements, Art. 7 CRA, and critical products with digital elements, Art. 8 CRA. Depending on the cybersecurity risk posed by a product, it is placed in one of the categories; the potential severity of the impact of a security incident, the number of potential victims or the number of other systems in the network to which an incident can spread play a role.[1575]

In contrast to the Directive on the sale of goods[1576] and the DID Directive[1577], which regulate **goods with digital content** in relation to B2C, the CRA is intended to apply to products with digital elements before they are placed on the market.[1578] According to the intention of the legislator, the provisions of the CRA will therefore only apply when the product is to be placed on the Union market.[1579] According to Art. 3 No. 21 CRA, such a **placing on the market** means the first 'making available' of a product with digital elements on the Union market. According to Art. 3 No. 22 CRA, any supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge, constitutes making available on the Union market.

The existence of an activity **in the context of a commercial activity** is therefore decisive. Products that are to be developed, tested or used within a company or university for research purposes or other non-commercial purposes are therefore not covered by the provisions of the CRA due to the lack of a business connection.[1580] However, as soon as (subsequent) distribution is planned as part of a commercial activity or simultaneous use of the product for both business and research purposes, the provisions of the CRA apply.[1581]

Open source software, i.e. free and open source software (Art. No. 48 CRA), which is distributed outside of a business activity, i.e. for non-commercial purposes, is also excluded.[1582] According to recital 18, this is the case if the software components are monetised. However, the mere financial support of

---

1572 Chiara, 3 *International Cybersecurity Law Review* 2022, 255 (256) et seq.
1573 Rec. 38 et seq. CRA.
1574 Rec. 40 et seq. CRA.
1575 Rec. 43, 45 et seq. CRA.
1576 Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects of the sale of goods, OJ L 136/28.
1577 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contracts for the supply of digital content and digital services, OJ L 136/1, 22.5.2019, p. 1-27.
1578 Voigt, P./Falk, L., *MMR* 2023, 88 (89).
1579 Rec. 1 CRA; Piltz, C./Weiß, A./Zwerschke, J., *CR* 2023, 155.
1580 Piltz, C./Weiß, A./Zwerschke, J., *CR* 2023, 155 (156).
1581 Piltz, C./Weiß, A./Zwerschke, J., *CR* 2023, 155 (156).
1582 Biendl, M./Füllsack, J., *CR* 2024, 378; Schöttle, H., *ZfPC* 2023, 215 (216).

the open source product should not be sufficient for the assumption of commercial activity.[1583] In contrast, open source software that is provided as part of a business activity is fully covered by the scope of the CRA.[1584]

bb) Personal scope

The obligations of the CRA are aimed at economic operators. According to Art. 3 No. 12 CRA, this is the manufacturer, the authorised representative, the importer, the distributor or any other natural or legal person who is subject to obligations in connection with the manufacture of products with digital elements or the making available on the market of products in accordance with this Regulation. The 'open source software steward' is a special case, Art. 3 No. 14 CRA.

A **manufacturer** is any person who develops or manufactures products with digital elements or has them designed, developed, manufactured and marketed under his name or trademark, Art. 3 No. 13 CRA. An entrepreneur is therefore also a manufacturer within the meaning of the CRA if he has development work carried out by external service providers or subcontractors and later places the product on the market under his own name or brand.[1585]

Authorised representative is a natural or legal person resident or established in the Union who has received a written mandate from a manufacturer to perform certain tasks on his behalf, Art. 3 No. 15 CRA.

According to Art. 3 No. 16 CRA, **an importer** is a natural or legal person resident or established in the Union who places a product with digital elements on the market in the Union under the name or trade mark of a natural or legal person resident or established outside the Union.

According to the legal definition of Art. 3 No. 17 CRA, **distributors** are natural or legal persons in the supply chain who make a product with digital elements available on the Union market without changing its nature, with the exception of the manufacturer or the importer.

cc) Temporal scope, Art. 69(2) CRA

According to Art. 69(2) CRA, the provisions of the regulation only apply to products with digital content that were placed on the market **36 months after the CRA came into force** and beyond.[1586] Products that were placed on the market before this date can still fall within the scope if they are then significantly modified physically or by a software update, Art. 69(2) CRA. A change to a product is considered to be substantial if it is made in such a way that the product no longer fulfils basic safety requirements or may deviate from an originally verified, intended purpose.[1587] In contrast, only minor changes to the source

1583 Rec. 18 CRA.
1584 Rec. 19 CRA.
1585 Rec. 78 CRA.
1586 Rec. 126 CRA.
1587 Rec. 38 CRA.

code and safety updates that do not change the intended purpose are not considered to be significant changes within the meaning of the CRA.[1588]

Special earlier periods of validity must be observed for the **reporting obligation** and the provisions on the notification of conformity assessment bodies: According to Art. 72(2) CRA, the former should apply after 21 months, while Art. 35 to 51 CRA regarding notification should apply from 18 months after the entry into force of the CRA.

dd) Area exceptions

The scope of the CRA is broad due to its horizontal approach. In order to avoid overlaps with existing vertical regulations, the CRA provides for numerous exemptions:

(1) Cloud provider

According to recital 12, the CRA should not apply to **cloud providers**. Although the term "cloud provider" is not specifically defined in the CRA, the definition contained in recitals 33 to 35 of the NIS 2 Directive can be considered.[1589] This refers to digital services that enable on-demand management and comprehensive remote access to a scalable and elastic pool of shared computing resources, even if these resources are distributed across multiple locations.[1590] Recital 12 CRA clarifies that cloud computing services should only fall within the scope of the NIS 2 Directive if they provide their services within the European Union and if they meet or exceed the threshold for medium-sized enterprises. It is unclear at this point whether companies below this threshold fall within the scope of the CRA or whether the NIS 2 Directive should apply to cloud providers.[1591]

In the case of digital services that do not fall under the definition of a **remote data processing solution** in Art. 3 No. 2 CRA, such as '**Software-as-a-Service' (SaaS), 'Platform-as-a-Service' (PaaS) or 'Infrastructure-as-a-Service' (IaaS)**, the NIS 2 Directive and its corresponding implementing legislation must be applied.[1592] The distinction between digital products and digital services is therefore likely to become more relevant in the future.[1593] If the manufacturer offers a product with cloud functions that allow the user to control it remotely, or if these cloud functions are an integral part of the product, such as a refrigerator with a digital shopping list or a smart thermostat, this is covered by the CRA regulations. However, if the functionality of a product is not supported or if the cloud service is designed or developed outside the responsibility of the manufacturer, the scope of the CRA does not apply.[1594]

1588 Rec. 39 CRA.
1589 Piltz, C./Weiß, A./Zwerschke, J., CR 2023, 155.
1590 Rec. 33 Directive (EU) 2022/2555.
1591 Piltz, C./Weiß, A./Zwerschke, J., CR 2023, 155.
1592 Biendl, M./Füllsack, J., *CR* 2024, 376 (379); Ruttloff, M./Wagner, F./Stilz, M., *BB* 2024, 1603 (1604).
1593 Dittrich, T./Heinelt, C., *RDi* 2023, 309 (311).
1594 Dittrich, T./Heinelt, C., *RDi* 2023, 309 (311).

(2) Exemptions for certain product groups, Art. 2(2) – (7), Art. 4(2) – (3) CRA

There are also exceptions for areas with more specialised regulations. According to Art. 2(2) CRA, these include products with digital elements that fall within the scope of the following provisions:

- Regulation (EU) 2017/745 on medical devices (a);
- Regulation (EU) 2017/746 on in vitro diagnostic medical devices[1595] (b) and
- Regulation (EU) 2019/2144 on type-approval of motor vehicles and of systems, components and separate technical units intended for such vehicles with regard to their general safety[1596] (c).

In addition, according to Art. 2(3) CRA, there is an exemption for products that have been certified in accordance with Regulation (EU) 2018/1139 on civil aviation rules (EASA Basic Regulation). Furthermore, Art. 2(4) CRA excludes devices from the scope of the CRA that fall under Directive 2014/90/EU on marine equipment.

A further exception to the scope applies to products with digital elements that have been developed or modified exclusively for national security or defence purposes and for the processing of classified information, Art. 2(7) CRA.

According to Art. 2(6) CRA, spare parts for products with digital elements are also excluded from the scope of the regulation if they are identical in design to the original inspected components.[1597]

An exemption in the broader sense can also be found in Art. 4(2) CRA: According to this, Member States are obliged to authorise the presentation or use of non-compliant products with digital elements, including prototypes, at trade fairs, exhibitions, demonstrations and similar events; the same applies to **unfinished software** that is made available for testing purposes for a limited period of time in accordance with Art. 4(3) CRA.[1598] For both product categories, a visible sign must be affixed indicating non-conformity with the CRA and the lack of authorisation to make them available on the market. Safety components that are mentioned in other Union legal acts are not covered by the exception, Art. 4(4) CRA.

At last, Art. 2(8) CRA clarifies that the CRA cannot oblige addressees of the regulation to provide information relating to the essential interests of the Member States in the area of national security, public security and defence.

[1595] Rec. 25 CRA.
[1596] Rec. 27 CRA.
[1597] Rec. 29 CRA.
[1598] Rec. 37 CRA.

d) General provisions of the CRA

With the CRA, the European legislator has opted for a '**risk-based approach**'.[1599] It assumes that all products with digital elements harbour a certain cybersecurity risk, although the intensity of this risk can vary greatly.[1600] In order to do justice to this variance, the regulator establishes risk categories and then links risk assessment procedures of varying intensity to this categorisation. This product classification system and the use of risk assessment procedures is similar to the procedure in other legal acts, such as the AIA[1601], the Medical Devices Regulation[1602], the General Product Safety Regulation.[1603]

aa) Categorisation of the cyber security risk

All products with digital elements must undergo a **cyber security risk assessment** and be categorised into one of **three risk levels.**

(1) Level 1: Products with digital elements, Art. 6 CRA

The **standard category** of products with digital elements includes all products that do not fall into the higher risk categories. The obligations are based on Art. 6 CRA. In the literature and here, the term 'normal products' is sometimes used.[1604] Further regulations must be observed from the next level onwards.

(2) Level 2: Important products with digital elements, Art. 7(1) in conjunction with Annex III CRA

The CRA introduces the category of **important products** in Art. 7(1) CRA. Annex III of the CRA lists the important products, subject to amendments, and divides them into two classes.[1605] Products are considered important if they have one of the core functionalities listed in Annex III.[1606]

The **devices listed in Annex III Class 1** include the following: Identity management systems and privileged access management software and hardware, including authentication and access control readers, such as biometric readers; stand-alone and embedded browsers; password management; software to detect, remove or quarantine malicious software; products with digital elements providing virtual private network (VPN) functionality; network management systems; security information and event management (SIEM) systems; boot managers; public key infrastructure and digital certificate issuing software; physical and virtual network interfaces; operating systems; routers, internet connection modems and switches; microprocessors with security-related functions; microcontrollers with security-related functionalities; application-specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA)

1599 Voigt, P./Falk, L., *MMR* 2023, 88 (90); more generally also Roth-Isigkeit, D., *MMR* 2024, 621.
1600 Also Rec. 28, 34 CRA.
1601 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, OJ L 2024/1689, 12.7.2024.
1602 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, OJ L 117/11, 5.5.2017, p. 1-175.
1603 Roth-Isigkeit, D., *MMR* 2024, 621 (623) et seq. with further references.
1604 Schweinoch, M./Meßner, D., *CR Report* 2022, R112 (R112).
1605 Rec. 44 CRA.
1606 Rec. 45 CRA.

with security-related functionalities; virtual assistants for the smart home and smart home products with security functions, including smart door locks, security cameras, baby monitoring systems and alarm systems.

Annex III Class II adds the **following important products**: Hypervisors and containerised runtime systems supporting virtualised execution of operating systems and similar environments; firewalls and intrusion detection and prevention systems; tamper-resistant microprocessors and tamper-resistant microcontrollers.

As these important Class I and II products pose higher risks in the event of a cybersecurity incident than normal products with digital elements, they are subject to stricter **conformity assessment procedures** within the provisions of the CRA.[1607] The products listed in Annex III are to be classified as important if they also fulfil at least one of the criteria in Art. 7(2) CRA. This is the case if the product with digital elements primarily fulfils functions that are critical to the cybersecurity of other products, networks or services, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection, Art. 7(2)(a) CRA.[1608] As a second criterion for classification as an important product with digital elements, Art. 7(2)(b) CRA cites the characteristic of the product that, through its central functions (e.g. network management, configuration control or virtualisation), is capable of disrupting, controlling or damaging many other devices or endangering the health and safety of users.[1609]

(3) Level 3: Critical products with digital elements, Art. 8 in conjunction with Annex IV CRA

Pursuant to Art. 8(1) CRA, the Commission is empowered to define **critical products with digital elements** within the meaning of **Annex IV** of the CRA by means of a delegated act (Art. 61 CRA). To be classified as a critical product, it must fulfil the core functions listed in Annex IV. The product must therefore have a cybersecurity function and pose a significant risk due to its intensity and ability to disrupt or damage other products.[1610] Such a product requires – in contrast to the important products – a special certificate in accordance with the requirements of Art. 46 et seqq. CSA. Currently, Annex IV CRA only includes hardware devices with security boxes, smart meter gateways in intelligent metering systems in accordance with the Internal Electricity Market Directive[1611], devices for secure crypto processing, smart cards and similar devices for advanced security purposes.

1607 Rec. 10, 44 CRA.
1608 Rec. 43 CRA.
1609 Rec. 43 CRA.
1610 Rec. 46 CRA.
1611 Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 concerning common rules for the internal market in electricity and amending Directive 2012/27/EU L 158/125 of 14.6.2019, p. 125-199.

bb) The different conformity assessment procedures

A direct consequence of the categorisation of products with digital elements into different risk levels is the different conformity assessment procedures that can or must be carried out depending on the risk level.[1612] The assessment procedures contained in the CRA are based on the modules of Decision No. 768/2008/EC[1613] from the 'New Legislative Framework'.[1614] In the same way, the CRA also favours self-regulation over preventive controls by the authorities.[1615] Four or three assessment procedures based on Modules A, B, C and H of the Decision have been included in Annex VIII. The procedures under Modules B and C build on each other and are applied in combination. The procedure according to module A for "normal" products is less strict while the stricter conformity assessment procedures are based on modules B, C and H. These procedures are stricter because a third party must necessarily be consulted, which thus gains an insight into the production process. In future, the legislator will specify the schemes for **cybersecurity certification**, which could be particularly attractive for practitioners due to certain privileges.

(1) The effect of the presumption of conformity, Art. 27 CRA

According to Art. 27(1) CRA, products with digital elements and processes of the manufacturer that comply with harmonised standards or parts thereof [...] are presumed to comply with the essential cybersecurity requirements set out in Annex I **(presumption of conformity)**.[1616] The presumption of conformity is therefore given if the product complies with harmonised standards within the meaning of Art. 27(1) CRA, common specifications pursuant to Art. 27(2) CRA **or** European cybersecurity certification schemes pursuant to Art. 27(8), (9) CRA.

Voluntary certification in accordance with the CSA therefore remains an option and is taken up again in the CRA.[1617] According to Art. 27(8) CRA, a declaration of conformity issued under another Union act may also give rise to a presumption of conformity, provided that this declaration covers the requirements of the CRA.

If the product fulfils the presumption of conformity, the manufacturer can demonstrate conformity and no further conformity assessment procedure is required.[1618]

1612 See only Rec. 10 CRA.
1613 Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products and repealing Council Decision 93/465/EEC.
1614 Rec. 91 CRA.
1615 Wiebe, G./Daelen, J., *EuZW* 2023, 257 (260) et seq.
1616 Rec. 79 CRA.
1617 Hessel, S./Callewaert, C., *K&R* 2022, 789 (793).
1618 Fellner, Normung für alle, p. 28; Piltz, C./Weiß, A./Zwerschke, J., CR 2023, 155 (161); Poncza, M., *ZfPC* 2023, 44 (49); Zirnstein, Y., *CR* 2022, 707 (712).

(2) The conformity assessment procedures in detail , Art. 32(1) – (4) CRA

The standard case for 'normal' products with digital elements is the risk assessment procedure based on **Module A** of Decision No. 768/2008/EC, Art. 32(1) CRA.[1619] This is carried out internally by the manufacturer on his own responsibility **without** control by a third party.[1620] The procedure includes (a) the preparation of technical documentation in accordance with Art. 31 CRA, Annex VII CRA, (b) ensuring the conformity of all design, development, manufacturing and vulnerability management processes within the requirements of Annex I Parts I and II CRA, (c) the preparation of a declaration of conformity for each product in accordance with Art. 28 CRA and (d) the affixing of the CE marking to each product, Art. 29 et seqq. CRA. Internal self-regulation only applies to products in the standard category, Art. 32(1) CRA.

Annex VIII CRA contains the EU type-examination procedure based on **Module B** of Decision No 768/2008/EC.[1621] In this sub-procedure, the conformity assessment is carried out by a notified body in accordance with Art. 35 et seqq. CRA. The manufacturer of the product with digital elements must apply to the notified body for testing, Annex VIII Part II No. 3 CRA. The body then checks a sample product from the manufacturer as well as the manufacturing process or the technical documentation. If the process fulfils the requirements of Annex I CRA and the sample has been developed in accordance with the manufacturing process checked by the body and also fulfils the requirements, the notified body then issues the conformity assessment. The risk assessment procedure is always carried out in combination with the internal production control in accordance with **Module C** of Decision No. 768/2008/EC, Annex VIII Part III CRA. Following the EU-type examination according to Module B, the manufacturer ensures the conformity of the series products with the EU-type (previously checked by the notified body) on the basis of an internal production control. This is regulated in Module C of Decision No. 768/2008/EC and is also listed in Annex VIII Part III of the CRA. In this part of the procedure, the manufacturer must take the necessary production and surveillance measures to ensure that the manufactured products conform to the type described in the EU type-examination certificate according to Module B.

Finally, **Module H** of Decision No. 768/2008/EC has also been included in Annex VIII of the CRA. In this risk assessment procedure, the manufacturer has a quality assurance system developed by him reviewed by the notified body of his choice by submitting an application to the body. This application must contain the technical documentation of the product categories and the actual quality assurance system. The system must fulfil the requirements of Annex VIII Part IV Number 3.2 CRA and in particular ensure that the essential requirements of Annex I CRA are guaranteed. The notified body then carries out audits of the manufacturer at regular intervals. During this conformity assessment procedure,

[1619] Rec. 91 CRA.
[1620] Annex VIII Part I para. 1 CRA.
[1621] Rec. 91 CRA.

the identification number of the notified body must also be affixed to the product after CE marking in accordance with Art. 30(4) CRA.

For this purpose, European schemes for cybersecurity certification are to be designated in future in accordance with Art. 27(9), Art. 61 CRA.[1622] These must first be adopted in accordance with Art. 46 et seq. CSA and can then also be used to demonstrate conformity qua presumption of conformity.[1623] The obligation to have a conformity assessment carried out by a third party (usually by the notified body) does not apply if a cybersecurity certificate has been issued for the product or process at a level of assurance of at least 'substantial' in accordance with the CSA.[1624] This certificate proves conformity regardless of the risk level of the product, Art. 27(8), (9) CRA. Additional obligations, such as detailed descriptions within the technical documentation in accordance with Annex VII No. 5 CRA, also no longer apply if a cybersecurity certificate has been issued. In most cases, it is likely to be advisable in practice to select the cybersecurity certificate at the 'substantial' assurance level. This covers all cases of the risk levels and also offers additional privileges. However, as no adopted schemes exist as yet, it remains to be seen how high the requirements of these procedures will be.

e) Rights and obligations of economic operators, Art. 13–26 CRA

In Articles 13–26, the CRA sets out a series of obligations that specifically address the individual economic operators. Manufacturers of products with digital content are subject to the most far-reaching obligations, as they can already influence product safety as part of the product design.[1625] Some general obligations are aimed at all economic operators in the CRA.

aa) General obligations

The obligation to cooperate with the market surveillance authorities applies to all economic operators, Art. 53 CRA.[1626] These authorities are established by the member states and are responsible for enforcing the CRA, Art. 52(2) CRA.[1627] In this concept, the market surveillance authority is similar to the national authorities that were introduced with the NIR Directive.[1628]

As part of the conformity assessment, all economic operators are obliged to grant the market surveillance authority access to all data and records required to assess the design, development, manufacture and vulnerability management of products with digital elements upon request, Art. 53, Art. 13(22), Art. 19 (7), Art. 14(6) CRA. In addition, economic operators must, upon request, provide the relevant authority with all names and addresses of economic operators from whom they have purchased products with

1622 Rec. 21 CRA.
1623 Rec. 81, 79 CRA.
1624 Rec. 9, 81 CRA.
1625 Wiebe, G., *ZRP* 2023, 73 et seq.
1626 Rec. 107 CRA.
1627 Rec. 120 CRA.
1628 Wagner, E./Holm-Hadulla, E./Ruttloff, M./Kappler, L./Bug, H., Metaverse und Recht, sec. 7 para. 471.

digital elements or to whom they have supplied such products. The economic operator must be able to retain and present this information for at least ten years, Art. 17 CRA.

bb) Obligations of manufacturers of products with digital elements

A **manufacturer** is any person who develops or manufactures products with digital elements or has them designed, developed, manufactured and marketed under their name or trademark, Art. 3 No. 18 CRA. An entrepreneur is therefore also a manufacturer within the meaning of the CRA if he has development work carried out by external service providers or subcontractors and later places the product on the market under his own name or brand.[1629]

cc) Obligations regarding the placing on the market, Art. 13 CRA

The central obligation for manufacturers is set out in Art. 13(1) CRA: "When placing a product with digital elements on the market, manufacturers shall ensure that the product has been designed, developed and manufactured in accordance with the essential requirements set out in Annex I, Part I.[1630] The provision is linked to the time of placing on the market. The requirements must therefore be met at this moment at the latest. As the product should also be designed and developed in accordance with the requirements of the CRA, the regulatory approach is described as 'security by design'.[1631]

(1) Product requirements, Annex I Part 1 CRA

According to Annex I Part I CRA, a product must fulfil the basic cybersecurity requirements.[1632] To this end, a level of security appropriate to the risk level of the product must be achieved, Annex I Part I (1) CRA.

More precisely, a product must be placed on the market **without known and exploitable vulnerabilities** and must also offer as few attack surfaces as possible in the case of external interfaces, Annex I Part I (2)(a), (j) CRA.[1633] Just in case, the product must be designed in such a way that the impact of an incident is minimised, Annex I Part I (2)(k) CRA.

The manufacturer must make the product available on the market with a **secure default configuration** and provide the options to reset the product to its **original state** and to safely and easily delete all data and settings in order to perform secure data migration, Annex I Part I (2)(b), (m) CRA.[1634]

The product must be able to be protected against emerging vulnerabilities by means of **security updates**, the installation of which is to be automatic unless the user deactivates this mechanism, Annex I Part I

1629 Rec. 78 CRA.
1630 Rec. 1, 10 CRA.
1631 Dittrich, T./Heinelt, C., *RDi* 2023, 309, (312); Heckmann, D./Ziegeler, N., *ITRB* 2024, 159 (160).
1632 Rec. 9 CRA.
1633 Rec. 54 CRA.
1634 Rec. 64 CRA.

(2)(c) CRA.[1635] Furthermore, the product must have a function for recording cybersecurity-relevant information, which also requires an opt-out mechanism, Annex I Part I (2)(l) CRA.[1636]

The product must be able to be **protected** against **unauthorised access** in accordance with Annex I Part I (2)(d) CRA, at least **by means of authentication, identity or access management systems**. In addition, the product must be able to detect and report unauthorised access. It is not clear from the wording of the standard whether this refers to a report to the user, the company or even an authority.

The confidentiality of personal data processed in connection with the use of the product must be guaranteed. The product must be protected against unauthorised access to data, commands, programs or configurations and any damage must be reported, Annex I Part I (2)(e), (f) CRA.

As with the GDPR, the principle of **data minimisation** applies to the processing of data. Annex I Part I (2)(g) CRA. In addition to the use of data, the impact of the product on the availability of other services should also be minimised, Annex I Part I (2)(i) CRA.

Basic and essential functions of the product must also be available after and during a safety incident, Annex I Part I (2)(h) CRA.

(2) Obligations after placing on the market, Art. 13(8) – (20) in conjunction with Annex I Part II CRA

The manufacturer's obligations continue even after the product has been placed on the Union market. Art. 13(8) CRA stipulates that **product vulnerabilities** that occur after the product has been placed on the market must be effectively addressed. The manufacturer must identify and document the vulnerabilities and components of the product, Annex I Part II No. 1 CRA. In addition, manufacturers are obliged to develop and provide suitable strategies and procedures, including concepts for the coordinated disclosure of vulnerabilities. These policies should be designed to allow the manufacturer to diagnose and fix the vulnerability before information can be disclosed to third parties.[1637] As a possible concept, manufacturers can implement so-called **bug bounty programmes** in which they provide incentives for reporting such vulnerabilities, as otherwise the high prices sometimes paid on the black market for vulnerability finders are more attractive.[1638] Examples include the 'Apple Security Bounty programme'[1639], the 'Microsoft Bug Bounty Programme'[1640] or 'Google's Bug Hunting community'[1641] .

In addition, the manufacturer must rectify such a vulnerability, for example by providing **security updates**, Annex I Part II No. 2 CRA. These must be made available and distributed immediately and free of charge in accordance with Annex I Part II No. 8 CRA. These obligations apply to the manufacturer

1635 Rec. 24, 56 CRA.
1636 Rec. 56 CRA.
1637 Rec. 77 CRA.
1638 Hessel, S./Callewaert, C., *K&R* 2022, 789 (792) et seq.
1639 https://security.apple.com/bounty (last accessed on: 1 November 2024).
1640 https://www.microsoft.com/en-us/msrc/bounty (last accessed on: 1 November 2024).
1641 https://bughunters.google.com/ (last accessed on: 1 November 2024).

for the expected lifetime of the product, but for a maximum period of five years after the product has been placed on the market, Art. 13(8) CRA.

Art. 13(13) CRA regulates a retention obligation for manufacturers. The technical documentation and the EU Declaration of Conformity must therefore be kept for at least 10 years after placing on the market and for a maximum of the support period.[1642]

The product must always be accompanied by instructions in simple language in digital or paper form.[1643] The instructions must contain all the information in Annex II CRA as well as the EU Declaration of Conformity or a link to it if it is only enclosed in simplified form, Art. 13(18), (20) CRA. The instructions must also contain the full address and contact details where the manufacturer can be contacted and name a central point of contact, Art. 13(16), (17) CRA.

Products with digital elements require a mark to identify them, such as a type, batch or serial number, Art. 13(15) CRA.

(3) Reporting obligations, Art. 14 CRA

As a concrete protection mechanism for IT security, the CRA, together with other European IT security legislation, above all the NIS 2 Directive, establishes an obligation to report vulnerabilities in products with digital elements to the bodies notified by the member states.[1644] The CRA imposes specific reporting obligations on manufacturers and other economic operators. In addition, the actors must also undertake vulnerability protection and take effective precautions around the reporting of vulnerabilities, Annex I Part I (2), (3)(k), Part II (1), (2), (4), (5), (6) CRA. The CRA thus subjects all economic operators to the so-called '**Coordinated Vulnerability Disclosure' (CVD)**[1645] concept and makes it a prerequisite for placing products with digital elements on the market through Part II of Annex I CRA.[1646]

Probably the most important and most onerous obligation for manufacturers once the product has been placed on the market is set out in Art. 14 et seq. CRA. According to Art. 14(1) CRA, the manufacturer has a **reporting obligation** with regard to **actively exploited vulnerabilities** (1) of the product manufactured by him with digital elements of which he becomes aware and with regard to **any serious incident** of which he becomes aware (3) and which has an impact on the security of the product.[1647] In principle, the notification must be made simultaneously to the **Computer Security Incident Response Team (CSIRT)** designated by the Member State as coordinator and to the **European Union Agency**

1642 Rec. 13 CRA.
1643 Rec. 18 CRA.
1644 Vettermann, O., *RDi* 2024, 260 (266).
1645 BSI guideline on the Coordinated Vulnerability Disclosure (CVD) process dated 1 December 2022, available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.pdf?__blob=publicationFile&v=4 (last accessed on: 1 November 2024).
1646 Vettermann, O., *MMR* 2023, 827 (830).
1647 Rec. 65 CRA.

for Cybersecurity (ENISA). The reports must be made via the standardised reporting platform (Art. 16 CRA).[1648]

(a) Notification of an actively exploited vulnerability, Art. 14(1) CRA

When reporting an actively exploited vulnerability, the manufacturer must comply with the following framework conditions:[1649]

The notification must be made immediately, i.e. without undue delay, and in any case within 24 hours of the manufacturer becoming aware of an actively exploited vulnerability, an early warning of the vulnerability, stating the Member States in which the product with digital elements was made available to its knowledge, Art. 14(2)(a) CRA.[1650]

The detailed notification of the exploited vulnerability must also be made as soon as possible, but in any case **within 72 hours** of the manufacturer becoming aware of it. The detailed notification shall include general information about the product, the nature of the exploitation of the vulnerability in question and any corrective and risk mitigation measures and countermeasures that users of the digital products can take. The manufacturer should also indicate how sensitive it considers the reported information to be, Art. 14(2)(b) CRA.

According to Art. 14(2)(c)(i) –(iii) CRA, a final report must be submitted **no later than 14 days** after a corrective or risk mitigation measure has been provided by the manufacturer. This must contain a description of the vulnerability, its severity and its impact (i). If available, the manufacturer must also provide information on the actor exploiting the vulnerability (ii). Finally, the final report must include information about the security updates that have been made available to address the vulnerability (iii).

These time limits correspond to those of the NIS 2 Directive, for example in Art. 23 Directive (EU) 2022/2555.[1651] Parallels can also be seen with the GDPR[1652]. According to Art. 33(1) GDPR, the notification of a data breach must also be made without undue delay and, if possible, within 72 hours.

(b) Notification of a serious incident, Art. 14(3) CRA

The manufacturer shall provide an early warning of a **serious incident** affecting the security of the product with digital content without undue delay and in any event within 24 hours of becoming aware of it.[1653] The early warning shall at least indicate whether the incident is suspected to be the result of unlawful or malicious acts, specifying the Member States in which the manufacturer's product was made available to its knowledge, Art. 14(4)(a) CRA.

1648 Rec. 65 CRA.
1649 Rec. 68 CRA.
1650 Rec. 66 CRA.
1651 Biendl, M./Füllsack, J., *CR* 2024, 376 (380).
1652 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
1653 Rec. 67 CRA.

The incident must be reported in detail immediately, but in any case within 72 hours of the manufacturer becoming aware of it. This notification shall include an initial assessment of the incident, corrective actions and remedial measures that users can take and, finally, an assessment of how sensitive the manufacturer considers the reported information to be, Art. 14(2)(b) CRA.[1654]

Within one month of the notification of the incident in accordance with (b), a final report must then be prepared in accordance with Art. 14(4)(c) CRA, which contains a detailed description of the security incident, including its severity and impact (i), as well as information on the nature of the threat or the underlying cause that probably triggered the security incident (ii) and information on the remedial measures taken and ongoing (iii).

(c) Addressee of the notification , Art. 14(1), (3) CRA

The notifications pursuant to Art. 14(1) and (3) CRA must in principle be made simultaneously to the Computer Security Incident Response Team (CSIRT) designated by the Member State as coordinator and to the European Union Agency for Cybersecurity (ENISA).[1655] The respective CSIRT to which the notification is to be addressed in addition to ENISA is determined in accordance with Art. 14(7) CRA.

According to Art. 14(7) CRA, the CSIRT to be addressed is the one designated by the Member State in whose territory the manufacturer has its main establishment. Art. 14(7) CRA stipulates that the place of main establishment is primarily located where the decisions relating to the cybersecurity of the manufacturer's products with digital elements are predominantly taken. Secondarily, if the Member State of the main establishment cannot be determined in the first way, the main establishment shall be located at the establishment of the manufacturer with the highest number of employees, Art. 14(2) CRA. If it is not possible to determine a main establishment within the Union using either of these approaches, the CSIRT to be addressed for the manufacturer is based on Art. 14(7) CRA. The notification must then alternatively be addressed to the CSIRT of that Member State,

- in which the authorised representative (Art. 18 CRA) of the manufacturer who acts for the majority of the manufacturer's products is established (a);
- in which the importer who places the majority of the manufacturer's products on the market is established (b);
- in which the distributor is established that provides the majority of the manufacturer's products on the Union market (c);
- Finally, the Member State in which the majority of users of the manufacturer's products are located (d).

In order to proceed, it is first necessary to maintain strict adherence to the established order of priority. In the event that the designated CSIRT cannot be determined with (a) can (b) be used and so on. The order of precedence is only broken if the manufacturer reports subsequent incidents after the first report

[1654] Rec. 71, 66 CRA.
[1655] Rec. 65 CRA.

to the CSIRT has been made in accordance with (d). In this case, the manufacturer may submit further reports to the same CSIRT in accordance with Art. 14(7) CRA. Conversely, this must mean that subsequent notifications in other cases are not to be sent to the CSIRT that was alerted first, but the addressee must be determined anew on the basis of Art. 14(7) CRA.

(d) Single reporting platform , Art. 16(1) CRA

Reporting in accordance with Art. 14(1) and (3) CRA is carried out via the standardised reporting platform referred to in Art. 16 CRA. Each Member State can provide an **endpoint for electronic reporting** via its CSIRT, which is then automatically distributed in the harmonised reporting platform.[1656]

ENISA is responsible for the establishment and ongoing operation of the standardised reporting platform in accordance with Art. 16(1) CRA.[1657] The reporting platform is used to disseminate information on cybersecurity risks within the European Union in order to facilitate the detection of known vulnerabilities in products.[1658] For example, in accordance with Art. 16(2) CRA, the CSIRT designated as coordinator, which originally receives a notification, forwards this notification via the standardised notification platform to all CSIRTs designated as coordinators in whose territory the product with digital elements was made available according to the manufacturer. However, the dissemination of the notification only takes place in principle. In exceptional circumstances, the dissemination of the notification can be postponed for as long as absolutely necessary for reasons of cybersecurity, Art. 16(2) CRA.[1659] The manufacturer expressly has the option of submitting an application and thus delaying dissemination. If the CSIRT decides in favour or grants the application, ENISA must be informed immediately. Reasons must be given for the delay and it must be stated when the distribution is expected to take place.

In addition to the complete postponement of dissemination, Art. 16(2) CRA allows only limited and general information about an exploited vulnerability to be provisionally disseminated to ENISA by the CSIRT contacted for the first time in particularly exceptional circumstances.[1660] The circumstances only need to be 'exceptional' for the full deferral, whereas Art. 16(2) CRA requires 'particularly exceptional' circumstances. To this end, the manufacturer must state in its notification pursuant to Art. 14(2) (b) CRA that a malicious actor has exploited the vulnerability only in the alerting Member State **and** that the dissemination would be contrary to the essential interests of the Member State **or** that the dissemination itself poses an immediate high security risk. Only the last two conditions are alternative.

According to Art. 16(6) CRA, a CSIRT designated as coordinator may, for legitimate reasons, postpone the dissemination of a notification of an actively exploited vulnerability for a period no longer than is

1656 Rec. 69 CRA.
1657 Rec. 72, 73 CRA.
1658 Rec. 66 CRA.
1659 Rec. 70 CRA.
1660 Rec. 71 CRA.

strictly necessary until the parties involved agree to the coordinated disclosure. However, this does not prevent the manufacturer from making a voluntary disclosure.[1661]

In addition to notifying the government authorities, if the manufacturer becomes aware of an actively exploited vulnerability or a serious incident, it must inform the affected users of the product with digital elements about the actively exploited vulnerability or a serious incident and about countermeasures that the users can take, in accordance with Art. 14(8) CRA. If the manufacturer fails to provide timely information, the CSIRTS designated as coordinators may make this information available to users if they consider this to be proportionate and necessary. The wording does not provide any information on the exact deadline, form and accuracy of the user information. In view of this legal uncertainty, a user-friendly approach is recommended in practice. Users should therefore be notified as early as possible, as precisely as possible and preferably by direct contact via email.

The CSIRTS also have the option of informing the public in accordance with Art. 17(2) CRA if awareness-raising is necessary to mitigate the consequences of the security incident.

dd) Obligations of importers and distributors of products with digital elements, Art. 19–22 CRA

In addition to manufacturers, the economic operators subject to the Cyber Resilience Act also include **importers** and **distributors of products with digital elements**. According to Art. 3 No. 16 CRA, an **importer** is a natural or legal person resident or established in the Union who places a product with digital elements on the market in the Union under the name or trademark of a natural or legal person resident or established outside the Union. According to the legal definition of Art. 3 No. 17 CRA, **distributors** are natural or legal persons in the supply chain who make a product with digital elements available on the Union market without changing its nature, with the exception of the manufacturer or the importer.[1662]

(1) Obligations of importers

The obligations of the **importer** are largely based on those of the manufacturer of a product with digital elements.[1663] According to Art. 19(1) CRA, the main obligation for importers is to prohibit the placing on the market of products with digital elements that do not comply with the essential requirements in Annex I Part I of the CRA. In accordance with Art. 19(2) CRA, importers must therefore check for themselves and ensure that the manufacturer has prepared the technical documentation, carried out an appropriate conformity assessment procedure, attached suitable instructions and affixed the CE marking. The importer must also affix or attach his contact details to the digital product (Art. 19(4) CRA). Like the manufacturer, the importer is also obliged to keep or submit the technical documentation and the EU declaration of conformity for a minimum period of 10 years after placing the product on the market,

1661 Rec. 74 CRA.
1662 Cf. Rec. 20, 78 et seq. CRA.
1663 Ruttloff, M./Wagner, F./Stilz, M., *BB* 2024, 1603 (1606).

limited by the length of the support period for the product, Art. 19(6) CRA. Finally, according to Art. 19(8) CRA, importers are obliged to inform the market surveillance authorities and, where possible, the end users of a product if a manufacturer of a product ceases operations and is consequently unable to fulfil the obligations of the CRA.

(2) Obligations of dealers

In comparison to the importer, the **distributor** only has to check whether the product is CE-marked, whether it is accompanied by instructions that fulfil the requirements of Annex II CRA, whether the manufacturer's declaration of conformity is available and whether the importer has included their contact details, Art. 20(2) CRA. However, a product may only be made available on the market if there is no reason to assume that neither the conformity of the product nor the procedure specified by the manufacturer fulfil the requirements of the CRA, Art. 20(3) CRA. At the reasoned request of the market surveillance authority, the distributor is also obliged to provide, in a language easily understood by the authority, all information and documentation necessary to demonstrate the conformity of the product and the procedures established by the manufacturer, and to co-operate with the authority to prevent cybersecurity risks, Art. 20(5) CRA. Finally, distributors, like importers, are obliged to notify the market surveillance authority in the event that the manufacturer of the product ceases operations, Art. 20(6) CRA. To summarise, a distributor is therefore not obliged by the provisions of the Cyber Resilience Act to maintain the conformity of the product with digital elements. However, they are nevertheless subject to such an obligation under the provisions of consumer warranty law for digital products in Sections 327d, 327e, 327f (1) BGB. [1664] This is where the CRA's judgements can then apply indirectly.[1665]

(3) Common obligations

According to Art. 19(5) CRA and Art. 20(4) CRA, both importers and distributors are obliged, if there is reason to believe that the conformity of a product is no longer given, to restore it or if this is not possible or the importer or distributor is unable to do so to withdraw the product from the market. Furthermore, if the manufacturer or importer discovers a ‘weak point’ in the product, they must inform the manufacturer of the product immediately. If the product poses a **significant cybersecurity risk** as a result of a vulnerability, the relevant market surveillance authority must be notified immediately, Art. 19(5) CRA or Art. 20(4) CRA. The ‘cybersecurity risk’ is defined in Art. 3 No. 37 CRA as "the potential for loss or disruption caused by a security incident, expressed as a combination of the magnitude of such loss or disruption and the likelihood of the security incident occurring". According to Art. 3 No. 38 CRA, such a risk is ‘significant’ if "due to its technical characteristics, it is likely to result in a security incident that could have a serious negative impact and cause significant material or immaterial loss or disruption". The draft Cyber Resilience Act does provide distributors and importers of a digital product with a detailed definition of a significant cyber security risk.[1666] However, this definition also contains

[1664] Rennert, J., *ZfDR* 2023, 206 (214) et seq.
[1665] Ruttloff, M./Wagner, F./Stilz, M., *BB* 2024, 1603 (1607) et seq.
[1666] See also Rec. 111 et seq. CRA.

various undefined legal terms and thresholds to be crossed, which must be assessed by the entrepreneurs and on the basis of which they must make a decision. However, as such an assessment entails a high liability risk for importers and distributors, in practice any incidents are likely to be reported.

However, according to Art. 21 CRA, importers and distributors are considered manufacturers of a digital product and are therefore subject to the obligations of Art. 13 and 14 CRA if they place the product on the market under their own name or trademark or if they significantly modify the product.[1667] According to Art. 22(1) CRA, this also applies if a natural or legal person is neither a manufacturer nor an importer nor a distributor, makes a substantial modification to the product and then places the product on the market.[1668] However, the person is only subject to the obligations set out in Art. 13 and Art. 14 CRA for the part of the product affected by the substantial modification or, if the substantial modification affects the cybersecurity of the product with digital elements, for the entire product, Art. 22(2) CRA.

ee) Special case: open source software stewards, Art. 24 CRA

The **developers and stewards of open source software**[1669] are subject to a significantly reduced catalogue of obligations compared to the manufacturers of digital products.[1670]

(1) Concept and special features of the scope

Free and open source software is software whose source code is openly shared and whose licence provides all the necessary rights to make it freely accessible, usable, modifiable and redistributable, Art. 3 No. 48 CRA. The draft still distinguishes between the supply phase and the development phase; if the provision of the software (supply phase) constitutes a business activity for the economic operator, the digital product is privileged as free and open source software, but is not completely excluded from the scope of the CRA by means of a sectoral exception.[1671] In the development phase, the type of activity or the method of financing is irrelevant and thus 'prototypes' never fall under the CRA.[1672]

An open source software component that is intended for integration into a product with digital elements by another manufacturer only falls within the scope of the Regulation if it is offered as part of a commercial activity. The fact that another manufacturer co-finances or supports the development of the software component is not in itself an indication of the commercial nature of the activity of the provider of the software component.[1673]

Software manufacturers who only contribute source code for free and open source software are completely excluded from the scope of the regulation if they are not subject to their responsibility.[1674] Open

1667 Rec. 79 CRA.
1668 Rec. 6, 39 CRA.
1669 For details on possible open source business models, see Poncza, M./Keppeler, L./Lennartz, M., *ZfPC* 2023, 117 (122).
1670 Heckmann, D./Ziegeler, N., *ITRB* 2024, 159 (160).
1671 Rec. 18 CRA; Schöttle, H., *ZfPC* 2023, 215 (216).
1672 Rec. 18 CRA.
1673 Rec. 18 CRA.
1674 Rec. 18 CRA.

source software that is ultimately designed for commercial activities, in particular the integration into commercial products with digital elements, is subject to the scope of the CRA with some privileges.[1675]

The obligations then fall to the the **open source software steward**, which the CRA introduces as a new category.[1676] This is a legal entity that is not a manufacturer, which has the purpose or objective of systematically and sustainably supporting the development of specific products with digital elements that are considered free and open source software **and** are intended for **commercial activities**, and which ensures the marketability of these products, Art. 3 No. 14 CRA.

(2) Voluntary control

In future, developers, users and other third parties will be able to have the conformity of open source software with the requirements of the CRA assessed voluntarily. According to Art. 25 CRA, delegated acts are to be issued for this purpose. Such a legal act could provide for a corresponding European scheme for cybersecurity certification in accordance with Article 48 of the CSA.[1677] According to Art. 32(5) CRA, manufacturers of open source software may undergo one of the conformity assessment procedures mentioned in Art. 32(1) CRA if the technical documentation of the product is made public at the time it is placed on the market.

(3) Obligations and exceptions for stewards

Art. 13(5) CRA stipulates that the manufacturer's duty of care to adapt the third-party software that is integrated into its own product to the security standard of Annex I CRA also applies if open source software is integrated.

Art. 24 CRA regulates the special obligations of the open source software stewards. According to Art. 24(1) CRA, the main obligation is to develop and document a strategy to support the effective handling and voluntary reporting of vulnerabilities in accordance with Art. 15 CRA and the development of a secure product in general. According to Art. 24(2) CRA, stewards must cooperate with the market surveillance authority and provide it with the documentation of the cybersecurity strategy described above upon request. This corresponds to the responsibility of the market surveillance authorities under Art. 52 (3) CRA to ensure the fulfilment of the administrator's obligations.

As for manufacturers, the obligations of Art. 14(1), (3) and (8) CRA also apply to stewards of open source software, Art. 13(6) CRA. The notification of actively exploited vulnerabilities is mandatory pursuant to Art. 14(1) CRA if the steward is involved in the development of a product with digital content, Art. 24(3) CRA. According to the definition in Art. 3 No. 1 CRA, this only applies if the product is placed on the market. According to Art. 24(3) CRA, a serious incident must be reported in accordance with Art. 14(3) CRA if the security incident leads to an impairment of the network and information

1675 Rec. 19 CRA.
1676 Biendl, M./Füllsack, J., *CR* 2024, 376 (378).
1677 Rec. 21 CRA.

systems provided by the steward for the development of products with digital elements.[1678] In this case, the users of the open source software must also be informed of the serious incident and, if necessary, provided with measures with which they can minimise the extent of the incident, Art. 14(8) CRA.

Stewards are exempt from the fines under Art. 64(3)–(10) CRA pursuant to Art. 64(10)(b) CRA. Stewards are not fined for every violation of the regulation.

f) Market surveillance, enforcement and sanctions

According to Art. 1(d) CRA, the regulation should also contain provisions on market surveillance, control and enforcement.

aa) Market surveillance and enforcement, Art. 52–60 CRA

The Member State market surveillance authorities are responsible for the market surveillance of products with digital elements and the enforcement of the provisions of the CRA; to this end, Art. 52(1) CRA declares the Market Surveillance Regulation[1679] to be applicable to products with digital elements within the meaning of the CRA.[1680] According to Art. 52(2) CRA, the Member States are obliged to designate one or more market surveillance authorities, whereby an existing authority can also be designated.[1681] Enforcement measures include the so-called 'sweeps'.[1682] According to Art. 60 CRA, market surveillance authorities are authorised to carry out 'sweeps' in which the manufacturer's products are purchased by the authorities under a pseudonym and tested for conformity with the CRA. The authorities of the Member States shall cooperate directly or through coordination by ENISA by means of joint actions to be made public, Art. 59(1), (5) CRA.[1683]

bb) Sanctions, Art. 64 CRA

The primary instrument used by market surveillance authorities to ensure enforcement is administrative sanction.[1684] These sanctions, which the authorities can impose on economic operators in the event of breaches of CRA obligations, are regulated in Art. 64 CRA. As a basic principle, Art. 64 (1) CRA states that sanctions must be effective, proportionate and dissuasive. The aspect of effectiveness is achieved with fines that are based on a percentage of the company's turnover and thus remain a deterrent even for large global corporations. Proportionality is achieved through a granular system of fines for different

1678 See Rec. 68 CRA.
1679 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ L 169, 25.6.2019, p. 1–44.
1680 Rec. 106 CRA.
1681 Rec. 107 CRA.
1682 Rec. 114 CRA.
1683 Rec. 33 CRA.
1684 Rec. 120 CRA.

breaches of obligation and, in accordance with Art. 64(5) CRA, through the final discretion of the authorities to apply a lower fine.[1685] In accordance with Art. 64(6) CRA, the market surveillance authority notifies the imposition of a fine to the authorities of the other member states. The authority may also levy processing fees, Art. 64(9) CRA. The sanction model is therefore comparable to the GDPR.[1686] This means in detail:

(1) Breaches of cybersecurity requirements in accordance with Annex I and Art. 13, 14, Art. 64(2) CRA

According to Art. 64(2) CRA, breaches of primary obligations under Art. 13 et seq. and Annex I CRA lead to fines of up to EUR 15 million. Companies pay up to 2.5 % of their global annual turnover in the previous financial year if this value exceeds EUR 15 million.

(2) Violations of Art. 18–53, Art. 63(3) CRA

For violations of Art. 18–23, 28, 30(1)–(4), Art. 31(1)–(4), Art. 32(1), (2) and (3), 33(5), Art. 39, 41, 47, 49 and 53 CRA, a fine of up to EUR 10 million or, in the case of companies, 2% of annual worldwide turnover is due in accordance with Art. 64(3) CRA.

(3) Incomplete, misleading or false information provided to the notified body or market surveillance authority, Art. 64(4) CRA

According to Art. 64(4), care must also be taken when responding to requests for information from the market surveillance authority and notified bodies. Incomplete, misleading or simply false information can be penalised with fines of up to EUR 5 million or up to 1% of a company's annual turnover. In addition, sanctions under the German UWG are also likely to be applicable to safety violations under the CRA.[1687]

(4) Exception for SMEs and administrators of open source software, Art. 64(10) CRA

However, according to Art. 64(10) CRA, the aforementioned fines do not apply to SMEs in the event of deadline violations pursuant to Art. 14(2)(a) and (4)(a) CRA. Stewards of open source software are completely exempt from the fines.

In addition to fines, there are also monitoring and intervention powers of public sector bodies, the power to withdraw despite compliance due to significant cybersecurity risks, Art. 54(1) CRA, and the prohibition in the event of formal non-compliance after an unsuccessful request for rectification, Art. 58(2), (1) CRA.

1685 Rec. 120 et seq. CRA.

1686 Wagner, E./Holm-Hadulla, E./Ruttloff, M./Kappler, L./Bug, H., Metaverse und Recht, sec. 7 para. 473, p. 151; Dittrich, T./Heinelt, C., *RDi* 2023, 309 (316); Schöttle, H., *ZfPC* 2023, 215.

1687 Weiden, H., *GRUR* 2024, 669 (673).

g) Summary and practical implications

With its first comprehensive and horizontal regulation of the cybersecurity requirements for digital products, the European Union has set out to achieve a major breakthrough. Binding cybersecurity requirements for products with digital elements are being introduced across the EU for the first time, with the aim of strengthening their resilience to cyberattacks and enabling consumers and companies to make more transparent decisions in a standardised internal market in terms of cybersecurity.

It must be recognised that the CRA, with its extremely extensive requirements for manufacturers, importers and distributors of digital products, creates a regulatory framework that can actually significantly reduce the risk of a cybersecurity flaw, even long after a product has been placed on the European market.[1688] This is because the CRA takes a promising approach to increasing the security of a digital product with the obligation to disclose vulnerabilities. The dense web of reporting obligations with the imposition of CVD obligations has the potential to improve consumer protection and product transparency in the Union.[1689] At the same time, the extensive reporting obligations pose a particular challenge for small and medium-sized companies.[1690] This will make it easier for market participants to assess the cybersecurity of a product and, in the long term, low-vulnerability and secure products are likely to prevail on the European single market.[1691]

The growing range of cyber-resilient products also reduces the strain for affected companies to implement the cybersecurity requirements of the NIS 2 Directive. This is because if only cyber-resilient products are available on the European market, only these can be used to fulfil the necessary **risk management obligations**.[1692] The Cyber Resilience Act must therefore be recognised as having the potential to raise the level of cybersecurity throughout the EU.[1693]

However, the various obligations for manufacturers, importers and distributors of digital products to increase cyber resilience are necessarily accompanied by a significant increase in compliance requirements.[1694] This is not limited to large market participants, but also includes small and medium-sized companies. Although this is essential for ensuring a high level of cybersecurity without restriction, it represents an additional expense for small companies.

The CRA's approach to reporting vulnerabilities and incidents has also been the subject of criticism. . In particular, the CRA requirements would create a real-time software database with open cybersecurity

---

1688 Biendl, M./Füllsack, J., *CR* 2024, 376 (383).
1689 Vettermann, O., *MMR* 2023, 827 (830).
1690 Dittrich, T./Heinelt, C., *RDi* 2023, 309 (314).
1691 Vettermann, O., *MMR* 2023, 827 (830).
1692 Cyber Resilience Act: EU strengthens cyber security of hardware and software, available at https://bdi.eu/artikel/news/cyber-resilience-act-eu-staerkt-cybersicherheit-von-hard-und-software (last accessed on: 1 November 2024).
1693 Biendl, M./Füllsack, J., *CR* 2024, 376 (383).
1694 Siglmüller, J., *ZfPC* 2023, 221 (222); Biendl, M./Füllsack, J., *CR* 2024, 376 (383).

vulnerabilities, which could present itself as an attractive target for hackers. In addition, the digital infrastructure would potentially become less secure, as cyber security vulnerabilities would be publicised before the affected companies could develop and provide patches and countermeasures. The Cyber Resilience Act would thus run counter to its own regulatory purpose of increasing the level of cyber security.[1695] However, the CRA can already partially refute this accusation, as Art. 16(2) CRA provides for the possibility of deferring the disclosure of reporting information in important cases. However, securing the reporting platform against cyberattacks remains a top priority due to the sensitivity of the information it contains.

Manufacturers should switch their processes to the requirements of the CRA as early as possible. It is true that most of the provisions of the CRA only become mandatory 36 months after entry into force (Art. 71 No. 2 CRA). However, as the requirements affect the fundamental design of a product, it is advisable for the stakeholders concerned to make decisions in this regard well in advance and, if necessary, to implement them, which can be a challenge for the obligated market participants due to some undefined legal terms in the CRA.

In order to facilitate the changes, the obligations under the draft regulation are summarised below. Six steps can be derived from the CRA in order to fulfil the obligations prior to placing on the market.

Step 1: A **cybersecurity risk assessment** must be carried out by the manufacturer as early as possible and, if necessary, updated during the course of development, Art. 13 (2), (4) CRA. In this assessment, the risk level of the future product is initially assessed by the manufacturer itself. Based on the result of this categorisation, the product should be designed in accordance with the safety requirements of the CRA from the outset. The law assumes that this step takes place or begins before the planning phase of the product (Art. 13(2) CRA). In practice, it is likely to be difficult to carry out a comprehensive analysis of cybersecurity risks if the specific dimensions of the product have not yet been determined. If the manufacturer is already required to carry out a risk assessment for its product under another more specific Union act, then it is sufficient if the manufacturer only carries out an overall assessment that fulfils the requirements of the other regulations and the CRA, Art. 13(4) CRA.

Step 2: Before the product can be placed on the market, the manufacturer must **prepare technical documentation** in accordance with Art. 31 CRA. It must contain the information listed in Annex VII CRA. The cybersecurity risk assessment must also be included in the technical documentation, Art. 13(4) CRA. In some cases, the technical documentation is also mentioned as part of the conformity assessment procedure in the modules in the Annex to the CRA. The duplication is only for editorial reasons, but the same documentation is meant.

[1695] Clasen, A., Cyber Resilience Act: Disclosure requirement concerns raised by experts, available at https://www.euractiv.com/section/cybersecurity/news/cyber-resilience-act-disclosure-requirement-concerns-raised-by-experts/ (last accessed on: 1 November 2024).

The technical documentation must describe how the manufacturer intends to fulfil the requirements of Annex I, Art. 31(1) CRA. This description is not required if the manufacturer includes a list of the applied harmonised standards, including the reference in the Official Journal, the common specifications and the European cybersecurity certification schemes that he uses, Annex VII No. 5 CRA. If the manufacturer uses one of these options, it also fulfils the requirements for the presumption of conformity in accordance with Art. 27 CRA.

The manufacturer must update the technical documentation during the support period. The technical documentation does not necessarily have to be carried out as a second step, but is mandatory before the product can be placed on the market, Art. 13(12) CRA. It is also a component of the majority of conformity assessment procedures. If the manufacturer believes that some of the essential requirements from Annex I Part I CRA are not applicable to their product, then a clear justification must be provided in the technical documentation for each requirement that is not fulfilled, Art. 13(3) CRA.

Step 3: The manufacturer must define a **support period** in accordance with Art. 13(8) CRA. This should correspond to the expected useful life of the product, but must last at least five years unless it can be assumed that the product will be in operation for less than five years, Art. 13(8) CRA. During the entire support period, the manufacturer must document and update the cybersecurity risk assessment, Art. 13(3) CRA. In addition, all security updates provided by the manufacturer during the support period must remain available for at least 10 years after the product is placed on the market and for a maximum of the support period, Art. 13(9) CRA. The end date of the support period must be easily visible on the product when it is purchased and must be specified at least to the month. With the introduction of the support period, the lifespan of a product now plays a major role in determining the period during which the manufacturer is obliged to provide support.[1696]

Step 4: A **conformity assessment procedure** in accordance with Art. 32 CRA must then be carried out. This involves checking the conformity of the product with digital elements and the procedures defined by the manufacturer with the requirements in Annex I. Depending on the risk of the product, more extensive conformity assessment procedures are provided for. In all cases, where available and applicable, conformity can be established by means of a European cybersecurity certification scheme in accordance with Art. 27(9) CRA qua presumption of conformity.

For normal products, the manufacturer has the choice of which conformity assessment procedure to carry out, Art. 32(1) CRA. He can choose between modules A, B, C and H.

For important and critical products, the manufacturer **cannot** demonstrate conformity through internal self-assessment (Module A). He only has the choice between EU type examination based on internal production control Art. 32(3)(a) CRA, Annex VIII Module B/C and comprehensive quality assurance,

[1696] Zirnstein, Y., *CRi* 2024, 65 (68).

Art. 32(3)(b) CRA, Annex VIII Module H. In the event of an increased cyber security risk, the involvement of third parties in the conformity assessment is therefore always necessary.[1697]

Step 5: If the selected conformity assessment procedure has demonstrated that the product and the procedure fulfil the essential requirements in Annex I Part I and II CRA, the manufacturer draws up the **EU declaration of conformity** (Art. 28 CRA) in accordance with Art. 13(12) CRA. The content of the declaration of conformity must correspond to the model in Annex V CRA, Art. 28(2) CRA. A single declaration is sufficient, which, however, then attests conformity with several Union legal acts, citing the relevant provisions (including the reference in the Official Journal), Art. 28(3) CRA.

Step 6: Finally, the **CE marking** (Art. 29 et seq. CRA) must be affixed to the corresponding product in accordance with Art. 13(12) CRA. The principles of CE marking according to Art. 30 of the Market Surveillance Regulation apply.[1698] Furthermore, if the product is covered by other EU acts that also require the affixing of a CE mark, it is sufficient to affix only one mark to the product, Art. 30(5) CRA.

1697 Rec. 92 CRA.

1698 Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Council Regulation (EEC) No 339/93.

4. Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554

Bibliography

Bernau, J., & Lutterbach, M., "Digital Operational Resilience Act (DORA): Paradigmenwechsel in der IT-Aufsicht," *BKR* (2023), 506; Clausmeier, D., "Die neue Verordnung des europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA)," *WM* (2022), 1861; Dittrich, T., & Heinelt, C., "Der Europäische DORA – neue Sicherheitsvorgaben für den Finanzsektor," *RDi* (2023), 164; Gronau, N., & Lindemann, M., Einführung in das Informationsmanagement, GITO mbH Verlag 2010; Hornung, G., & Schallbruch, M. (eds.), IT-Sicherheitsrecht – Praxishandbuch, 2nd ed., Nomos 2024; Roth-Isigkeit, D., "Der risikobasierte Ansatz als Paradigma des Digitalverwaltungsrechts," *MMR* (2024), 621; Siglmüller, J., "Cyber Resilience Act und Digital Operational Resilience Act – Lässt sich IT-Sicherheit rechtlich erzwingen?" *ZfPC* (2023), 221; Pohle, J., "DORA: Die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor," *VersR* (2023), 273; Voigt, P., & Ritter-Döring, V., "Der Digital Operational Resilience Act – Sektorspezifische Anforderungen an die digitale Resilienz von Finanzunternehmen," *CR* (2023), 82; Waschbusch, G., Schlenker, B., & Kiszka, S., IKT-Risiken und Bankenaufsichtsrecht – Eine Analyse der regulatorischen Anforderungen an das IKT-Risikomanagement in Banken unter besonderer Berücksichtigung der BAIT und des DORA, 1st ed., Nomos 2023.

a) Preliminary considerations

aa) Introduction and background to the regulation

The EU is facing an ever-increasing threat from cyberattacks. Many of these cyberattacks also target the critical infrastructure of the financial sector and can therefore jeopardise the stability of the financial system.[1699] The threat of financial instability is reached when the financial system is no longer able to fulfil its essential economic functions, such as the processing of payment transactions.

In 2022, a digital disaster was declared in Germany for the first time after a ransomware attack, a form of digital blackmail, hit the state.[1700] But it is not only public institutions that are becoming the target of cyberattacks. More and more actors are focussing their efforts on private, often smaller, companies. More than half of all German companies now feel that their existence is threatened by cyberattacks,[1701] particularly in view of the increasing amounts of damage caused by these attacks.[1702]

1699 Rec. 1, 3 of Regulation (EU) 2022/2554.

1700 BSI, Die Lage der IT-Sicherheit in Deutschland 2022, available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022-Doppelseite.html?nn=129410 (last accessed on: 1 November 2024).

1701 German Association for Information Technology, Telecommunications and New Media (BITKOOM) on economic protection 2023, p.12 available at https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf (last accessed on: 1 November 2024).

1702 German Association for Information Technology, Telecommunications and New Media (BITKOOM) on economic protection 2023, p.4, available at https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf (last accessed on: 1 November 2024).

In view of the risks to the European financial system outlined above, the European legislator felt compelled to create the first legal requirements for digital operational resilience and the protection of information and communication technology (ICT) in the financial sector with the **Digital Operational Resilience Act (DORA).**[1703] The term ICT covers all technologies that are suitable for storing, processing or communicating data. This also includes the way in which this data is used and all associated services.[1704] One example of ICT in the financial sector is cloud computing services such as the *IBM* 'Financial Transaction Manager'[1705], which are used by financial institutions to process financial transactions and analyse data.

DORA pursues the overarching goal of strengthening the European financial market against cyber risks.[1706] The growing interconnectedness between companies, even across national borders, increases the risk of cyber incidents, which can spread to the entire financial system.[1707] DORA is intended to achieve these goals by creating obligations that apply to all financial companies.[1708] This should prevent companies from making short-term savings just to secure a supposed competitive advantage.[1709]

DORA entered into force on 16 January 2023 and will become directly applicable on 17 January 2025 after the 24-month implementation period in accordance with Art. 64 DORA.

bb) Relationship to other European cybersecurity law

DORA initially contains overlaps with the requirements of the NIS 2 Directive, for example with regard to (ICT) risk management, communication in the event of a security incident or sanctions, whereby the requirements for financial companies set out in DORA are more stringent than the requirements of the NIS 2 Directive.[1710] In this respect, both legal regimes are in a relationship of speciality, as Art. 4(1) Directive (EU) 2022/2555 clearly states.[1711] It follows that financial undertakings covered by DORA cannot also be regarded as institutions within the meaning of the NIS 2 Directive and therefore do not have to comply with the obligations of the NIS 2 Directive or the national implementing legislation that apply to institutions.[1712]

1703 Rec. 1 - 4 Regulation (EU) 2022/2554; Scott, H., The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies, Program on International Financial Systems, p. 12, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904113 (last accessed on: 1.11.2024).

1704 Gronau, N./Lindemann, M., p.15.

1705 IBM Financial Transaction Manager, available at https://www.ibm.com/de-de/products/financial-transaction-software (last accessed on: 1 November 2024).

1706 Rec. 1, 3 Regulation (EU) 2022/2554; Scott H., The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies, Program on International Financial Systems, p. 12, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904113 (last accessed on: 1 November 2024).

1707 Dittrich, T./Heinelt, C., *RDi* 2023, 164.

1708 Hornung G./Schallbruch M./Bomhard, D./Siglmüller J., IT Sicherheitsrecht, Section 29 para. 11.

1709 Dittrich, T./Heinelt, C., *RDi* 2023, 164 (171).

1710 Rec. 16 Regulation (EU) 2022/2554.

1711 See also Rec. 28 of Directive (EU) 2022/2555.

1712 https://www.openkritis.de/it-sicherheitsgesetz/NIS 2-umsetzung-gesetz-cybersicherheit.html#changes (last accessed on: 1 November 2024).

b) Scope, Art. 2 DORA

The sector-specific scope of the regulation results from Art. 2 DORA and exclusively covers the **financial undertakings enumerated** in Art. 2(1), (2) DORA**.** According to Art. 2(1) DORA, this includes the following companies:

- Credit institutions (a);
- Payment institutions, including payment institutions exempted under Directive (EU) 2015/2366 (b);
- Account information service provider (c);
- Electronic money institutions, including electronic money institutions exempted under Directive 2009/110/EC (d);
- Investment firms (e), providers of crypto services authorised under the Regulation on Markets in Crypto Securities and issuers of value-referenced tokens (f);
- Central securities depository (g);
- central counterparties (h);
- trading venues (i);
- trade repository (j);
- Alternative investment fund managers (k);
- Management companies (l);
- Data provision services (m);
- Insurance and reinsurance companies (n);
- Insurance intermediaries, reinsurance intermediaries and insurance intermediaries in secondary employment (o);
- Institutions for occupational retirement provision (p);
- rating agencies (q);
- Administrators of critical reference values (r);
- Swarm financing service provider (s);
- securitisation register (t) and
- ICT third-party service providers (u).

The term "**ICT third-party service provider"** within the meaning of Art. 2(1)(u) DORA includes companies that provide ICT services in accordance with the definition in Art. 3 No. 19 DORA.[1713]

However, the groups of companies listed in Art. 2(2) DORA are expressly excluded from the scope .

In order to exempt **micro-enterprises** from the sometimes far-reaching obligations and burdens of the DORA, the regulation stipulates exemptions and special features in various places.[1714] According to Art.

[1713] Rec. 29 et seq. VO (EU) 2022/2554.
[1714] Rec. 21, 38 Regulation (EU) 2022/2554.

3 No. 60 DORA, micro-enterprises within the meaning of the DORA are companies that employ fewer than 10 people and have an annual turnover or balance sheet of less than EUR 2 million.

In some cases, micro-enterprises are completely exempt from individual obligations, for example from certain test procedures in Art. 26(1) DORA. In other cases, there are modifications compared to the requirements for larger financial companies, such as in Art. 12(4) DORA. However, according to their wording, some obligations also apply in full to micro-enterprises, such as the obligation to identify critical ICT assets pursuant to Art. 8(4) DORA.

Of course, this does not apply to micro-enterprises, which are already excluded from the scope by Art. 2(3)(e) DORA.

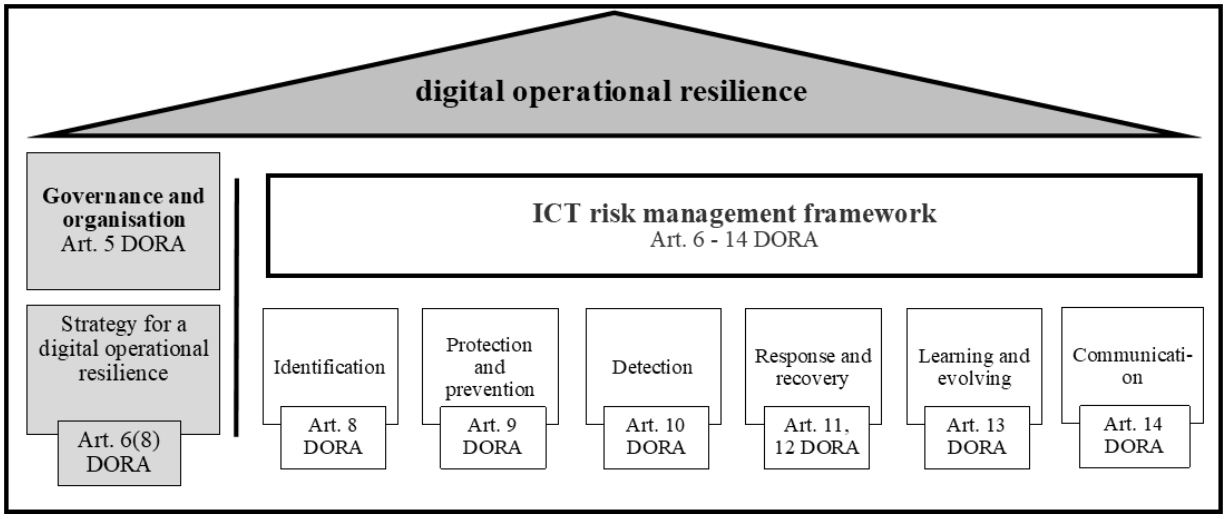
c) Obligations for financial companies, Art. 5–35 DORA

DORA contains a number of obligations for financial organisations, which can be divided into the following five categories: ICT risk management, aa); ICT incident reporting, bb); digital operational resilience testing, cc); ICT third-party manager, dd); and reporting and monitoring, ee).[1715] The obligations for financial companies set out in Art. 5–35 DORA must be implemented in accordance with Art. 4(1), (2) DORA, taking into account the **principle of proportionality**, which is why the size, risk profile and type and complexity of the services of the respective company must always be taken into account appropriately. Although the principle of proportionality is a principle codified in primary law (Art. 5(4) TEU), the legislator considered a separate regulation to be necessary in view of the broad scope of the DORA.[1716] The principle of proportionality is also the dogmatic basis for the risk-based approach that the Union legislator consistently pursues in digital legislation, which is also reflected in Art. 4 DORA.[1717]

aa) Obligations under the ICT risk management framework , Art. 5–14 DORA

Art. 5(1) DORA obliges financial undertakings to introduce an internal governance and control framework that ensures effective and prudent management of ICT risks in accordance with Art. 6(4). The obligations of financial companies with regard to ICT risk management, governance and organisation can be described as follows:

[1715] Rec. 47 Regulation (EU) 2022/2554.
[1716] Voigt, P./Ritter-Döring, V., *CR* 2023, 82 (83); Clausmeier, D., *WM* 2022, 1861 (1862).
[1717] Rec. 13 Regulation (EU) 2022/2554; on the risk-based approach, see Roth-Isigkeit, D., *MMR* 2024, 621.



Source: Waschbusch, G., Schlenker, B., & Kiszka, S., IKT-Risiken, p.129

(1) Organisational duties of the management body, Art. 5(2) DORA

Art. 5(2) DORA declares the definition, authorisation, monitoring and responsibility for all arrangements relating to ICT risk management to be the task of the management body of the financial undertaking[1718]. The **management body** is legally defined in Art. 3 No. 30 DORA with reference to Art. 3(1) No. 7 Capital Requirements Regulation[1719]: This is to be understood as the body of the respective company that has been appointed in accordance with the provisions of national law and has the authority to determine the strategy, objectives and principles of the institution, as well as to monitor and control the decisions of the management. In addition, this body should include the persons who actually manage the institution.[1720] Accordingly, the governing body of financial institutions is usually the management in the form of the managing director or management board.[1721]

Art. 5(1)(a)–(i) DORA specifies this catalogue of tasks to the effect that the management body of a financial undertaking bears ultimate responsibility for the management of ICT risks (a) and is responsible for introducing guidelines to ensure high standards with regard to the availability, authenticity, integrity and confidentiality of data (b). As Art. 5(1)(a) DORA transmissions the ultimate responsibility for ICT risk management to the management body, this duty can no longer be delegated.[1722] In addition to the advantage of better justiciability, it may also make sense from a business perspective, as the management should ideally have an overview of both the business and internal structures and obligations within a company structure.[1723]

In addition, clear roles and responsibilities for ICT-related functions and governance arrangements for effective communication and coordination must be defined (c). Furthermore, the management body is

1718 Rec. 47 Regulation (EU) 2022/2554.
1719 VO (EU) 2013/36/EU.
1720 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.126.
1721 Clausmeier, D., *WM* 2022, 1861 (1862).
1722 Hornung, G./Schallbruch, M./Bomhard, D./Siglmüller, J., IT Sicherheitsrecht, Sec. 29 para. 29 et seq.
1723 Clausmeier, D., *WM* 2022, 1861 (1862).

responsible for defining and approving the digital operational resilience strategy and the company's risk tolerance threshold **(**d**)**. The management body approves, monitors and regularly reviews the ICT business continuity guidelines and the ICT response and recovery plans, which are integrated into the general business continuity plans (e**)**. In addition, the governing body reviews internal ICT audit plans (f) and ensures that sufficient budget resources are allocated to meet the requirements of digital resilience, including training and awareness programmes for ICT security (g). It also monitors the agreements with third-party ICT providers, approves the relevant guidelines and ensures the establishment of internal reporting channels to be properly informed about agreements, changes and incidents related to third-party ICT providers (h), (i).

(2) Duty of the management body to provide further training, Art. 5(4) DORA

Art. 5(4) DORA stipulates the obligation of all members of the management body to attend regular training sessions with the aim of actively maintaining sufficient knowledge and skills up to date at all times. The provision is similar to Art. 20(2) Directive (EU) 2022/2555 and serves the purpose that the management must have a certain level of expertise in order to be able to properly assess and consequently guarantee compliance with the requirements within the meaning of Art. 5(2) DORA.[1724]

(3) Obligation to update for ICT systems, protocols and tools, Art. 7 DORA

Art. 7 DORA initially contains technical requirements for ICT systems and protocols or other tools. To protect against cyberattacks in a constantly changing digital threat situation, it is necessary to keep all systems up to date with updates, Art. 7 DORA. in this respect, DORA also follows the 'security by design' approach.[1725]

According to Art. 7(a)–(c) DORA, the protocols and tools of financial organisations must comply with the proportionality principle of Art. 4 DORA, be reliable and have sufficient capacity, including for peak operations. Only a system that is as up to date as possible can respond appropriately quickly to attacks.[1726] According to Art. 7(d) DORA, these systems must therefore also be technologically resilient in order to be able to work even under heavy load, such as in cases of above-average call-off rates.[1727]

(4) Identification of ICT risks, Art. 8 DORA

As a first preventive measure against ICT incidents, Art. 8 DORA specifies the obligation to identify potential threats and ICT vulnerabilities. According to Art. 8(2) DORA, this includes the recording of risk scenarios. This obligation includes the identification of risks emanating from other financial companies as well as any risks in the company's own operations that could affect other financial companies. The reviews should be carried out at least once a year. In addition, Art. 8(4), 5 DORA obliges companies to keep a record.

1724 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.128; Dittrich, T./Heinelt, C., *RDi* 2023, 164 (166).
1725 Hornung, G./Schallbruch, M./Bomhard, D./Siglmüller J., IT Sicherheitsrecht, Section 29 para. 21; Dittrich, T./Heinelt, C., *RDi* 2023, 164 (166).
1726 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.132.
1727 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.132.

(5) Protection and prevention of incidents, Art. 9 DORA

In order to optimally protect themselves from damage caused by security incidents, companies must use appropriate ICT security tools, policies and procedures in accordance with Art. 9(1) DORA. This includes, in particular, general '**business continuity management' (BCM).** These are management procedures that regulate how a company's employees should behave in the event of an incident that restricts operations in order to maintain business continuity.

Art. 9(2) DORA contains the obligation to ensure secure data transmission through high standards with regard to the availability, authenticity, integrity and confidentiality of data. This is achieved through the creation of an information security guideline, which should contain rules to fulfil the protection objectives.[1728]

The protection and prevention objectives are to be achieved through ICT solutions and processes in accordance with Art. 9(3) DORA. The article contains requirements for these solutions and processes in (a)–(d). These requirements are secure data transmission, protection against data corruption, unauthorised access and technical defects, availability and protection against data management-specific risks.[1729]

(6) Recognition mechanisms, Art. 10 DORA

In accordance with Art. 10(1) DORA, financial companies are also obliged to introduce mechanisms to identify potential vulnerabilities and security gaps as a preventive measure. According to Art. 3 No. 16 DORA, a vulnerability is any point within an asset, system, process or control that makes it vulnerable to attack. To ensure that these mechanisms work in an emergency, they must also be tested regularly in accordance with Art. 10(1), (2) DORA using the procedures listed in Art. 25 DORA.

(7) Response to incidents, Art. 11 DORA

The creation of comprehensive ICT business continuity guidelines is an explicitly stated component of the ICT risk management framework in Art. 11(1) DORA.[1730] According to Art. 11(2) DORA, these guidelines are to be implemented through special regulations, procedures and mechanisms, which in turn are to be precisely documented. The purpose of creating the ICT business continuity guidelines is to ensure the continuation of the important functions of the financial company by creating an 'emergency concept'[1731] in the event of ICT-related incidents and to prevent the occurrence of damage by reacting quickly and appropriately, see Art. 11(2)(a), (b) DORA. In addition, Art. 11(4) DORA stipulates that the ICT business continuity guideline must continue to be maintained and tested after its creation, particularly with regard to critical and essential functions that have not been outsourced by the financial company itself but to third-party ICT service providers.

1728 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.136.

1729 Rec. 47 Regulation (EU) 2022/2554.

1730 Hornung, G./Schallbruch, M./Bomhard, D./Siglmüller, J., IT Sicherheitsrecht, Section 29 para. 23.

1731 Cf. wording of BaF regarding Minimum Requirements for Risk Management AT 7.3, available at https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs1021_MaRisk_Erlaeuterungen.pdf?__blob=publicationFile&v=5 (last accessed on: 1 November 2024).

The testing obligation is also precisely standardised in Art. 11(4) DORA, according to which annual testing and a renewed test following fundamental changes to the ICT systems is provided for. The same testing obligation applies to the crisis communication plans also mentioned in Art. 14 DORA, although Art. 11(4)(b) DORA does not specify the frequency of the tests.

(8) Guidelines and procedures for backup, recovery and restoration, Art. 12 DORA

The obligations under Art. 11 DORA are supplemented by Art. 12 DORA, which describes the procedure following an ICT incident: According to Art. 12(1)(a) DORA, companies are obliged to develop and document guidelines and procedures that regulate the company's data security. In addition, according to Art. 11(1)(b) DORA, there is an obligation to define procedures and methods for the recovery and restoration of lost data. This is intended to minimise the downtime (or recovery time)[1732]. In concrete terms, this means that companies are obliged to define a backup strategy that specifies which data must be backed up and how often. According to Art. 12(1) DORA, however, these backup systems must not compromise the security or usability of IT systems and must be tested regularly to ensure that they are functioning properly. Finally, the obligation to check the integrity of the data after an ICT incident in accordance with Art. 12(7) DORA must be observed. According to the wording of the standard, this is done by means of multiple checks and comparisons of the data from the checks.

(9) Further development obligation, Art. 13 DORA

According to Art. 13 DORA, companies also have an internal development obligation. According to Art. 13(1) DORA, sufficient capacity must be provided to document information on possible system vulnerabilities, cyber threats and ICT-related incidents. The ICT risk management framework is to be further developed through the documentation and the findings from the incidents.[1733] The retrospective review is also intended to determine whether previously defined procedures were followed and whether the selected defence measures were effective during an incident, Art. 13(2) DORA. The measures taken are to be assessed, among other things, according to the speed of response, as well as the effectiveness of determining the impact of ICT incidents and internal and external communication.

The results from the assessment following an incident are incorporated into an ICT risk assessment process in accordance with Art. 13(3) DORA, in which the results from the tests in accordance with Art. 26, 27 DORA must also be included. In accordance with Art. 13(5) DORA, senior ICT employees must report to the management body of the respective company once a year on the findings obtained and make recommendations for action.

In addition, Art. 13(6) DORA contains the obligation to provide mandatory training for employees to raise awareness of ICT security.

1732 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.143.

1733 Hornung, G./Schallbruch, M./Bomhard, D./Siglmüller, J., IT Sicherheitsrecht, § 29 para. 24; Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.145.

(10) Communication plans, Art. 14 DORA

As the final part of the ICT risk management framework, Art. 14(1) DORA also requires the reporting of serious ICT incidents or vulnerabilities to customers, other financial organisations and the public. To this end, companies are obliged to draw up crisis communication plans to enable responsible disclosure.[1734] In addition, Art. 14(2) DORA requires an internal communication strategy towards a company's employees and external stakeholders.[1735]

Finally, Art. 14(3) DORA requires the appointment of a person to implement the communication strategy for ICT-related incidents, who should act as a kind of "emergency spokesperson" to represent the company to the public.[1736]

bb) Simplified ICT risk management framework, Art. 16 DORA

Art. 16 DORA contains a restriction of the obligations just described within the ICT risk management framework for certain types of companies; Art. 5 to 15 DORA do not apply to these types of companies.

Art. 16(1) DORA initially regulates the applicability of simplified ICT risk management for small and non-interconnected investment firms. These are investment firms that fulfil the requirements of Art. 3 No. 34 DORA in conjunction with Art. 11(1) Investment Firms Regulation . [1737]

In addition, the simplified ICT risk management framework applies to certain payment institutions in accordance with Art. 32(1) PSD2[1738], certain electronic money institutions that are excluded from the scope of the Electronic Money Directive[1739] and small institutions for occupational retirement provision.

cc) ICT third party risk management, Art. 28–30 DORA

Art. 28 et seq. DORA contain obligations regarding the handling of financial companies with **ICT third parties**. According to Art. 28(1) DORA, **ICT third-party service providers** should be treated as part of ICT risk management. This is based on the idea that by outsourcing, companies take on a risk that they cannot control themselves with regard to the emergence of ICT risks. To avoid these risks, the handling of third-party ICT service providers should be defined in advance by systems and methods.[1740] In accordance with Art. 28(1)(a) DORA, the responsibility for compliance with the obligations under the Regulation remains fully with the financial undertaking even when outsourcing to ICT third parties.

In addition, before a contractual agreement on the use of ICT services is concluded, a comprehensive risk analysis should be carried out, taking into account the far-reaching substantive requirements of the Regulation, see Art. 28(4) DORA.

1734 Rec. 32 Regulation (EU) 2022/2554; Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.147.
1735 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.147.
1736 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.147.
1737 VO (EU) 2019/2033/EU.
1738 DIRECTIVE (EU) 2015/2366/EU.
1739 DIRECTIVE (EU) 2009/110/EC.
1740 Voigt, P./Ritter-Döring, V., *CR* 2023, 82 (88).

Art. 30 DORA also obliges companies to ensure compliance with certain minimum contractual content regarding the use of ICT services. However, the requirements mentioned in Art. 30(2) DORA are not fundamentally new, but are based on existing requirements for outsourcing contracts, in particular with regard to critical or essential functions and agreements with cloud providers.[1741]

d) ICT-related incidents - handling and reporting, Art. 17–19 DORA

According to Art. 3 No. 8 DORA, an **ICT-related incident** is an event or a corresponding series of related events not planned by the financial company that affect the security of the network and information systems and have a negative impact on the availability, authenticity, integrity or confidentiality of data or on the services provided by the financial company.

Companies have an obligation to report **serious ICT-related incidents** to the responsible higher financial level. In addition, the management must be informed of the incident in accordance with Art. 1(1)(a)(ii) DORA. According to the definition in Art. 3 No. 10 DORA, an ICT-related incident is serious if it can have a far-reaching negative impact on the network and information systems that fulfil the critical or important functions of a company.

The severity level is determined on the basis of criteria previously defined by the company. If a materiality threshold is exceeded according to these criteria, the incident is categorised as serious.[1742]

So-called **cyber threats** are to be distinguished from serious ICT-related incidents. According to Art. 3 No. 12 DORA, cyber threats describe a possible event or action that could damage, disrupt or in any way impair network and information systems, their users and other persons.

The reporting of cyber threats is only carried out on a voluntary basis and only from a certain level of materiality, Art. 1(1)(a)(ii) DORA. The differentiation in the wording of the law makes it clear that the term ICT-related incident is to be understood more broadly than a "cyber attack" or “cyber threat”. [1743] This usually originates from malicious actors outside the company. The broad term, on the other hand, also includes incidents caused unintentionally by employees.[1744]

e) Testing digital resilience through test programmes, Art. 24–27 DORA

aa) Basic testing obligation, Art. 24 DORA

In addition to the obligations arising from the ICT risk management framework, DORA also contains the obligation in Art. 24 et seq. DORA to regularly test digital resilience.[1745]

The audit is always carried out by independent parties, so-called ‘testers’ in accordance with Art. 24(4) DORA, whereby these may be internal or external persons. In the case of an internal audit,

1741 Bernau, J./Lutterbach, M., *BKR* 2023, 506 (512).
1742 Clausmeier, D., *WM* 2022, 1861 (1863).
1743 Dittrich, T./Heinelt, C., *RDi* 2023, 164 (167).
1744 Dittrich, T./Heinelt, C., *RDi* 2023, 164 (167).
1745 Rec. 56 et seq. VO (EU) 2022/2554.

companies must ensure that sufficient financial resources are available for the audit and that no conflicts of interest arise during the audit.[1746] Further requirements for the selection of testers are set out in Art. 27 DORA. Special regulations apply to micro-entrepreneurs, Art. 24(4) et seqq. DORA.

In principle, Art. 24(3) DORA stipulates that financial companies can determine the appropriate scope and frequency of the audits themselves. The standard to be applied here is based on a risk-based approach according to the size of the company, how great the risk of attacks is for the company in question and how high the company's need for protection is. This again represents a manifestation of the proportionality principle.

If problems or vulnerabilities are found during such a test, Art. 24(5) DORA also stipulates the obligation to draw up procedures and guidelines for dealing with such problems, such as the prioritisation or classification of deficiencies, and how these can be remedied. Due to the lack of legal references, it can be concluded that companies can independently determine the frequency with which digital resilience tests are carried out, taking into account the risk-based assessment.

However, an exception to this is the testing of any ICT systems or ICT applications that support critical or other important functions within the meaning of Art. 24(6) DORA. According to Art. 24(6) DORA, these must be appropriately tested once a year.

bb) Threat-Led Penetration Tests, Art. 25–27 DORA

In addition, there is a requirement for certain types of companies to carry out further, threat-oriented tests in accordance with Art. 25(1) DORA.

Part of these are also so-called '**threat-led penetration tests**' (TLPTs).[1747] These are threat-orientated penetration tests in accordance with Art. 3 No. 17 DORA. The TLPTs are intended to simulate a threat that is as close to reality as possible, enabling a live production test of the critical systems.

TLPTs must be completed by this type of company at least every three years in accordance with Art. 26(1) DORA. In principle, TLPTs can be carried out by both internal and external testers in the same way as tests in accordance with Art. 24 DORA. However, Art. 26(8) DORA stipulates that every third TLPT must be carried out by an external tester.

The provision that the obligation to carry out TLPTs only applies to those companies that are exposed to the greatest risk according to a risk-based assessment once again represents an expression of the proportionality principle within the DORA.[1748] If the tests have been carried out properly in accordance with Art. 26, 27 DORA, the competent authorities must issue the company with a certificate to this effect. However, this means that full responsibility remains with the company management.[1749]

1746 Pohle J., *VersR* 2023, 273 (278).
1747 Rec. 43, 56 Regulation (EU) 2022/2554.
1748 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.151.
1749 Pohle, J., *VersR* 2023, 273 (278).

f) Supervision, enforcement and sanctions, Art. 46 et seqq. DORA

DORA establishes in Art. 46 et seqq. a comprehensive supervisory system for critical ICT service providers in the financial sector at European level for the first time.[1750] According to Art. 46(a)–(q) DORA, the responsibility of the authority depends on the type of financial undertaking.[1751] Art. 47 DORA regulates the cooperation between the authorities responsible under DORA and the structures and authorities created by the NIS 2 Directive. In particular, the exchange of information and the possibility of coordinating supervisory activities and inspections in connection with critical ICT third-party service providers are defined in order to ensure effective cooperation and rapid response mechanisms.[1752] Art. 48 DORA contains the obligation for the authorities to exchange information (2) and to cooperate (1).[1753]

aa) Supervision and enforcement, Art. 46, 47 DORA

Both national and European authorities are responsible for the supervision of and compliance with the provisions of the DORA. While the national supervisory authorities are responsible for monitoring financial companies with regard to the implementation of the regulation, carrying out inspections and imposing sanctions in accordance with Art. 46 DORA, the EBA, ESMA and EIOPA are responsible for cross-border matters at European level. These authorities are also responsible for the supervision of critical third-party ICT service providers in order to ensure uniform application of the regulations in the European Union (Art. 47 DORA).

In addition, critical third-party ICT service providers that provide essential services for financial companies are subject to centralised supervision by specialised supervisory authorities. These authorities work in close co-operation with national and European authorities to ensure the stability and resilience of these services (Art. 35 DORA). The competent authorities have extensive enforcement powers, ranging from ordering corrective measures to imposing sanctions, to ensure the digital operational resilience of financial institutions (Art. 50 DORA).

bb) Sanctions, Art. 50–54 DORA

(1) Administrative sanctions, Art. 50 DORA

Art. 50 DORA first describes the supervisory, investigative and sanctioning powers of the administrative authorities.

The triad of offences against DORA, as described in Art. 50(3) DORA, already corresponds to the principles known from the GDPR and the NIS 2 Directive. Accordingly, sanctions or other measures in the event of infringements must always be effective, proportionate and dissuasive.[1754]

1750 Hornung, G./Schallbruch, M./Bomhard, D./Siglmüller, J., IT Sicherheitsrecht, Section 29 para. 39.
1751 Hornung, G./Schallbruch, M./Bomhard, D./Siglmüller, J., IT Sicherheitsrecht, Section 29 para. 39.
1752 Rec. 80, 97 Regulation (EU) 2022/2554.
1753 Rec. 18 Regulation (EU) 2022/2554.
1754 Dittrich, T./Heinelt, C., *RDi* 2023, 164 (169).

In addition, Chapter VII of the DORA also sets out obligations that must be fulfilled by the administrative authority itself. If the competent administrative authority imposes sanctions against infringements, the authority must publish each decision in accordance with Art. 54(1) DORA on its official website. It must be possible to identify the person committing the offence from the publication in accordance with Art. 54(2) DORA and comprehensive information on the offence must be provided. In addition to the sanctions, this obligation to publish creates a kind of "pillory effect" through the public announcement.[1755]

However, DORA does not contain a corresponding catalogue of fines. Corresponding catalogues of fines should rather be drawn up by the competent national financial authorities such as BaFin, see Art. 50–52 DORA.[1756]

(2) Criminal sanctions, Art. 52 DORA

Art. 52 DORA also sets out the possibilities of criminal sanctions. It is still unclear how criminal liability for violations of DORA affects the management of a company. In contrast to the NIS 2 Directive, the DORA itself does not contain a catalogue of fines or other criminal sanctions. Rather, according to the regulation, the national legislator should be free to establish criminal sanctions for violations of DORA.[1757]

g) Conclusion

aa) Summary

DORA contains regulations for previously unresolved issues of sector-specific financial cybersecurity law. Above all, it contains abstract and theoretical regulations for the updating obligations of IT service providers.[1758] To counteract the excessive demands placed on companies, familiar regulatory techniques such as the proportionality principle have been incorporated into the regulation.[1759]

DORA makes it illegal to delegate cyber monitoring to third parties. According to Art. 5(2) DORA, the monitoring obligation is not transmissionable; management bears sole responsibility and cannot delegate it, which can be seen as a disproportionately serious interference in the company structure. It appears questionable whether management can adequately fulfil the numerous obligations under the ICT risk management framework. It is precisely the purpose of effective corporate management that tasks within the company can be delegated to specialised third parties for maximum effectiveness.[1760] In theory, the training obligation under Art. 5(5) DORA is intended to ensure that company management acquires the

1755 Dittrich, T./Heinelt, C., *RDi* 2023, 164 (169).
1756 Rec. 81 Regulation (EU) 2022/2554.
1757 Pohle, J., *VersR* 2023, 273 (282).
1758 Siglmüller, J., *ZfPC* 2023, 221 (224).
1759 Clausmeier, D., *WM* 2022, 1861 (1862).
1760 Siglmüller, J., *ZfPC* 2023, 221 (223).

necessary expertise. In addition, the responsibility for cybersecurity has also been anchored in corporate management through the 'G7 Fundamental Elements of Cybersecurity for the Financial Sector'.[1761]

There is also the aforementioned overlap with the BAIT regulations. Difficulties are caused by the different designation of requirements, which means that a detailed comparison of the individual obligations under BAIT and DORA is necessary, which represents a high level of effort for the companies.[1762]

Finally, there are obligations to carry out TLPTs, Art. 26 DORA. The costs of carrying out these tests are high. The preparation and follow-up work also requires up to one year, which makes the rigid three-year deadline for the next round appear disproportionately early.[1763]

bb) Practical guide

As the DORA is a regulation, it has a direct regulatory effect and, unlike the NIS 2 Directive, for example, does not need to be transposed into German law first.
Therefore, all the obligations described above will apply directly from 17 January 2025. There is therefore no further transitional period for adapting existing contractual agreements. Companies must therefore have already reformed their digital compliance strategy.
Even before the DORA obligations come into force, the regulations on the AI systems of financial companies in accordance with the "banking supervisory requirements for IT" (BAIT)[1764] must also be observed. There are many points of overlap between the existing requirements of BAIT and the obligations under DORA. It can therefore be assumed that at least the German banks already meet the requirements of DORA.[1765]

1761 Clausmeier, D., *WM* 2022, 1861 (1862); https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf (last accessed on: 1 November 2024).
1762 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.159; Dittrich, T./Heinelt, C., *RDi* 2023, 164 (165).
1763 Clausmeier, D., *WM* 2022, 1861 (1864).
1764 BaFin IT requirements for banks in accordance with Circular 10/2017, available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171106_BAIT.html (last accessed on: 1 November 2024).
1765 Waschbusch, G./Schlenker, B./Kiszka, S., IKT-Risiken, p.159, 160.

II. Regulation on Artificial Intelligence - Regulation (EU) 2024/1689

Bibliography

Ashkar, D., & Schröder, C., "Das Gesetz über künstliche Intelligenz der Europäischen Union (KI-Verordnung)," *BB* (2024), 771; Becker, D., & Feuerstack, D., "Die EU-KI-Verordnung – Überblick und Bewertung der finalen Fassung der KI-VO," *KIR* (2024), 62; Bomhard, D., & Siglmüller, J., "AI Act – das Trilog-Ergebnis," *RDi* (2024), 45; Bronner, P., "Die KI-Verordnung (KI-VO) der EU," *jurisPR-ITR* 13/2024; Chibanguza, K., & Steege, H., "Die KI-Verordnung – Überblick über den neuen Rechtsrahmen," NJW (2024), 1769; Ebers, M., Hoch, V., Rosenkranz, F., Ruschemeier, H., & Steinrötter, B., "Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf – Eine kritische Bewertung durch Mitglieder der Robotics & AI Law Society (RAILS)," *RDi* (2021), 528; Förster, A., & Gehrmann, M., "Die KI-Verordnung aus HR-Sicht," *SPA* (2024), 113; Frost, Y., Steiniger, M., & Vivekens, S., "Nutzen, Chancen, Risiken und Haftung bei der Verwendung von Künstlicher Intelligenz im Kontext der KI-Verordnung und KI-Haftungsrichtlinie," *MPR* (2024), 4; Geradin, D., Karanikioti, T., & Katsifis, D., "GDPR Myopia: How a well-intended regulation ended up favouring large online platforms - the case of ad tech," *European Competition Journal*, Vol. 17 (2021), 47; Gerdemann, D., "Konformitätsbewertung als Kernpflicht der KI-Verordnung," NJW (2024), 2209; Hacker, P., & Berz, A., "Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick," *ZRP* (2023), 226; Honer, M., & Schöbel, P., "Das Gesetz über Künstliche Intelligenz im System der europäischen Digitalregulierung – Ein Überblick," *JuS* (2024), 648; Krahn, N., "The European Union's Artificial Intelligence Act – A Status Report," *TLJ* (2024), 120; Kraul, T. (ed.), Das neue Recht der digitalen Dienste – Digital Service Act, Nomos 2023 ; Krönke, C., "Das europäische KI-Gesetz: Eine Verordnung mit Licht und Schatten," *NVwZ* (2024), 529; Lachenmann, F., "EU-Rat stimmt KI-Verordnung zu – neue Pflichten für Unternehmen," *MMR-Aktuell* (2024), 01359; Lachenmann, F., & Meyer, J., "Die Richtlinie über KI-Haftung – Beweislasterleichterungen für durch KI-Systeme entstandene Schäden," *MMR-Aktuell* (2023), 457000; Martini, M., & Wendehorst, C. (eds.), KI-VO – Verordnung über künstliche Intelligenz – Kommentar, 1st ed., C.H. Beck 2024; Möller-Klapperich, J., "Die neue KI-Verordnung der EU," *NJ* (2024), 337; Pilniok, A., "Unionsrechtliche Regulierung des Einsatzes von KI-Systemen in der öffentlichen Verwaltung," *DÖV* (2024), 581; Roth-Isigkeit, D., "Der risikobasierte Ansatz als Paradigma des Digitalverwaltungsrechts – Die KI-VO im Kontext europäischer Risikoregulierung," *MMR* (2024), 621; Schwartmann, R., Keber, T., & Zenner, K. (eds.), KI-Verordnung – Leitfaden für die Praxis, 1st ed., C.F. Müller 2024; Steinrötter, B. (ed.), Europäische Plattformregulierung, 1st ed., Nomos 2023; Steege, H., & Chibanguza, K., Metaverse, 1st ed., C.H. Beck 2023; Wegener, B., Europäische Querschnittpolitiken – Enzyklopädie Europarecht, Band 8, 2nd ed., Nomos 2021; Voigt, P., & Hullen, N. (eds.), Handbuch KI-Verordnung – FAQ zum EU AI Act, Springer 2024; von Welser, T., "Die KI-VO – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz," *GRUR-Prax* (2024), 485; Wendt, J., & Wendt, D., "Einigung auf Rechtsrahmen für Künstliche Intelligenz in der EU: AI Act," *ZfPC* (2024), 86; Wendt, J., & Wendt, D., Das neue Recht der Künstlichen Intelligenz, Nomos 2024.

1. Introduction

a) Background to the regulation of artificial intelligence

The growing importance of artificial intelligence in various areas of the economy and everyday life is also leading to a growing need for a groundbreaking legal framework for this technology — at least this

is the perspective in the European Union, where the Artificial Intelligence Act (AIA)[1766] has now created the world's first comprehensive set of regulations for the application of artificial intelligence. [1767]

Prior to this, the Commission presented an **AI strategy**[1768] on 25 April 2018, which called for a corresponding guarantee of an ethical and legal framework. The White Paper on AI[1769] published in February 2020 then set out initial plans for the regulation of so-called 'high-risk' applications in certain sectors. The Commission finally presented a concrete draft law in April 2021.[1770] This draft already contained a risk-based approach according to which AI systems are categorised into different risk levels. The European Parliament's subsequent draft in June 2022[1771] provided for a number of amendments and additions, including in particular the introduction of the 'basic model' as an additional AI system category. Following the EU Council's draft in November 2022 and the subsequent trilogue negotiations, the Parliament finally adopted the regulation by a large majority on 13 March 2024. The Council of the EU also adopted the regulation on 21 May 2024 and it was published in the Official Journal of the European Union on 12 July 2024. The Regulation entered into force 20 days after publication in the Official Journal on 1 August 2024 and applies — with a few exceptions — 24 months after the date of entry into force.

The legal nature of the AIA has remained the same across the various drafts and negotiations: it is a preventive prohibition law that prohibits the use of AI in numerous application scenarios or makes it dependent on technical, organisational and legal requirements.[1772] This, in turn, is based on a risk-based approach which, depending on the risk of the AI system, provides for a complete ban or varying degrees of strictness and labelling and transparency obligations. The focus is on the technological neutrality of the regulatory approach, according to which it is not the AI system per se that is taken into account, but the potential risk of the specific application of an AI system.[1773] The regulatory framework has become considerably extensive: 180 recitals can be used to interpret 113 articles in 13 chapters. In addition, there are 13 annexes and 68 definitions in Article 3 of the AIA.

b) Objectives and recitals

With the AIA, the European Union hopes to play a pioneering role worldwide in the introduction of safe, trustworthy and ethically acceptable AI.[1774] According to the subject matter of the Regulation under

---

1766 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation), OJ L 144, 12.7.2024, p. 1.

1767 Krahn, N., *TLJ* 2024, 120; Möller-Klapperich, J., *NJ* 2024, 337 (338).

1768 COM(2018) 237 final.

1769 COM(2020) 65 final.

1770 COM(2021) 206 final.

1771 European Parliament, Amendments of the European Parliament of 14 June 2023 to the Act on Artificial Intelligence and amending certain Union acts (COM(2021) 206 - C9-0146/2021 - 2021/0106(COD)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_DE.html.

1772 Bomhard, D./Siglmüller, J., *RDi* 2024, 45.

1773 Wendt, J./Wendt, D., *ZfPC* 2024, 86.

1774 Rec. 2, 8 Regulation (EU) 2024/1689.

Art. 1(1) of the AIA and the explanations in numerous recitals, the Regulation is intended in particular to

- improve the functioning of the internal market through a harmonised legal framework for the development, placing on the market, commissioning and use of artificial intelligence systems in the EU;
- promote the deployment of human-centred and trustworthy AI while ensuring the protection of health, safety and fundamental rights enshrined in the Charter of Fundamental Rights of the European Union, including democracy, the rule of law and environmental protection; and
- Ensure protection against the harmful effects of AI systems in the Union while supporting innovation.

How these objectives are achieved by the AIA is summarised in Art. 1(2) of the AIA. These include:

- harmonised rules for the placing on the market, putting into service and use of AI systems in the Union;
- Prohibition of certain AI practices;
- specific requirements for high-risk AI systems and obligations for actors in relation to such systems;
- harmonised transparency rules for certain AI systems;
- harmonised rules for the placing on the market of AI models for general purposes;
- Rules for market surveillance, market supervision, governance and enforcement;
- Measures to promote innovation, with a particular focus on SMEs, including start-ups.

c) Demarcations

In addition to the AIA, the European legislator has launched a number of other legislative initiatives that essentially focus on the regulation of artificial intelligence, albeit with different orientations. While the AIA aims to provide AI developers and providers with clear requirements and obligations in relation to the specific use of AI, other projects focus primarily on liability for AI. For example, the **Product Liability Directive** is being revised in order to address the special characteristics of AI, particularly with regard to complexity, autonomy and opacity, in the context of strict liability for damages.[1775] In addition, the AI Liability Directive is adapting provisions on non-contractual civil liability with the same objective.[1776]

In addition to the distinction from liability law requirements, it should be noted that although the AIA does not affect other data law provisions such as the Data Act, certain overlaps can be identified: For example, Art. 10(1) of the AIA contains provisions on requirements for data sets and data governance

[1775] Draft 2022/0302(COD) in its latest version of 14 January 2024.
[1776] Draft 2022/0303(COD) of 28.9.2022.

for high-risk systems. As large amounts of personal data are also regularly required for AI systems, the scope of the GDPR also applies in many cases.[1777]

2. Scope and definitions

For the scope of the Regulation, a distinction must be made between the AI systems covered by the material scope of the AIA (Art. 3 No. 1 AIA), the controllers covered by the personal scope and the territorial scope.

a) Material scope

aa) AI systems, Art. 3 No. 1 AIA

The Regulation primarily applies to **AI systems**. What AI systems are within the meaning of the Regulation was defined in Art. 3 No. 1 of the AIA. According to this, the term 'AI system' means a

> "… machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;".

According to this definition, six criteria can be summarised:[1778] The system is machine-supported (1), designed for autonomous operation (2) and adaptable (3). In addition, the system can derive (5) explicit or implicit goals (4) from the inputs, whereby the results can influence the physical or virtual environment (6).

Firstly, it should be noted that the characteristics of the machine-supported system or the programme's influence on the environment are not yet very meaningful and encompass almost every computer programme.[1779] The decisive criterion for differentiating between AI systems and conventional programmes, however, is the **extent of autonomy**.[1780] Autonomy is understood to mean that an AI system acts independently of human intervention to a certain extent and is able to work without human intervention.[1781] The characteristic of the adaptability of an AI system after commissioning refers to "its ability to learn, through which it can change during its use"[1782].

The material scope of the AIA is therefore extremely broad and has often been criticised due to its lack of definitional clarity.[1783] However, despite the broad definition, the term can often be analysed together

---

1777 For a detailed explanation of the relationship between the AI Regulation and the GDPR, see Schwartmann, R./Keber, T./Zenner K., AI Regulation, Part 2, Chapter 1, para. 34 et seq.

1778 Schwartmann, R./Keber, T./Zenner, K., KI-VO, Part 2, Chapter 1, para. 13.

1779 Bomhard, D./Siglmüller, J., *RDi* 2024, 45; Ebers, M./Hoch, V./Rosenkranz, F./Ruschemeier, H./Steinrötter, B, *RDi* 2021, 529.

1780 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, Section 2 para. 12; Bomhard, D./Siglmüller, J., *RDi* 2024, 45; Förster/Gehrmann, *SPA* 2024, 113 (114); Möller-Klapperich, *NJ* 2024, 337 (338).

1781 Rec. 12 Regulation (EU) 2024/1689.

1782 Rec. 12 Regulation (EU) 2024/1689.

1783 See only Steinrötter, B./Bastians, H., Europäische Plattformregulierung, Section 21 para. 6; Möller-Klapperich, J., *NJW* 2024, 337, 339.

with the recitals and the technical understanding, so that in practice there will probably be less legal uncertainty than initially feared.[1784] A guideline being developed by the Commission will also serve as a concrete aid to interpretation (Art. 96(1)(f) of the AIA). Until such a guideline is available, detailed explanations of the OECD definition can also be used, which is in line with the Regulation but is not legally binding in the EU.[1785]

However, the exact interpretation of this term and any difficulties in practice remain to be seen. In practice, assuming a low-risk strategy, it should be assumed to be an AI system in cases of doubt, just to be on the safe side.[1786]

bb) AI models with general purpose, Art. 3 No. 63 AIA

In addition to AI systems, **general purpose AI models** (**GPAI**[1787]) are also covered by the scope of the AIA, Art. 2(1)(a) AIA. AI models with a general purpose are defined in Art. 3 No. 63 of the AIA: According to this, an AI model with a general purpose is:

> " … an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market;"

However, the term AI model itself is not explicitly defined. An approximation of the term AI model is possible by distinguishing it from the term AI system. The distinction between AI models and AI systems can be found in recital 97 of the AIA: According to this, AI systems, in contrast to AI models, have additional components, such as user interfaces.[1788] Consequently, AI models are usually integrated into AI systems and are essential elements of these. AI models can therefore also exist on their own. In simplified terms, the AI model could be regarded as the AI itself, while the AI system describes the product intended for the end user.[1789] If one focuses on the explicitly mentioned component of the user interface, one could, using the example of *OpenAI* products, consider 'ChatGPT' as an AI system and the programme behind it in the form of *GPT-4/GPT-3* etc. as an AI model.[1790]

1784 Bomhard, D./Siglmüller, J., *RDi* 2024, 45.

1785 Schwartmann, R./Keber, T./Zenner, K., KI-VO, Part 2, Chapter 1, para. 12, 15; see also the explanations of the OECD definition at https://www.oecd-ilibrary.org/science-and-technology/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.

1786 Bomhard, D./Siglmüller, J., *RDi* 2024, 45.

1787 GPAI is an acronym for the English word *General Purpose AI Model*. Alternatively, the term *Foundation Model* is also used. In terms of content, both terms refer to AI models with a general purpose. See Schwartmann, R./Keber, T./Zenner, K., KI-VO, Part 2, Chapter 1, para. 16.

1788 Rec. 97 Regulation (EU) 2024/1689.

1789 Bomhard, D./Siglmüller, J., *RDi* 2024, 45 (50).

1790 Bomhard, D./Siglmüller, J., *RDi* 2024, 45 (50).

The provisions in the Regulation then refer to models that have a general purpose. This is a core element of the definition in Art. 3 No. 63 AIA. The general purpose is largely determined by the ability to competently fulfil a wide range of different tasks.[1791] Typical examples of such AI models are large generative AI models such as *GPT-4*, *Claude 3* or *Llama 2*, which can flexibly generate content and map a wide range of different tasks.[1792]

b) Personal scope

The personal scope primarily includes the operator involved in the AI value chain, namely the **providers of** the AI system.[1793] In some cases, the deployer and, in certain cases, the importers, distributors, authorised representatives, the notified body or the end user are also affected. The corresponding definitions can be found in Art. 3 No. 3–8 of the AIA.

aa) Provider, Art. 3 No. 3 AIA

According to the relevant definition, a *provider* is a natural or legal person, public sector body, agency or other body which develops or has developed an AI system or an AI model with a general purpose and places it on the market under its own name or trade mark or puts the AI system into service under its own name or trade mark, whether in return for payment or free of charge. The term “provider” is therefore largely similar to the term "manufacturer" in other legal acts, such as Art. 3 No. 8 GSP Regulation.[1794]

bb) Deployer, Art. 3 No. 4 AIA

In contrast, a *deployer* is a natural or legal person, public sector body, institution or other body that uses an AI system under its own responsibility, unless the AI system is used in the context of a personal and non-professional activity.

Nowadays, companies have more and more opportunities to operate AI systems under their own responsibility. Accordingly, many companies will fulfil the status of operator, so that they are included in the personal scope of the regulation.[1795]

c) Territorial scope

The territorial scope is regulated in Art. 2(1) of the AIA and follows the **market place principle**. According to Art. 2(1)(a) of the AIA, the Regulation applies to providers that place on the market or put into service AI systems or general purpose AI models in the Union, regardless of whether these providers are established or located in the Union or in a third country. Operators of AI systems are affected under Article 2(1)(b) of the AIA if they are established in the Union (principle of establishment). What is

1791 Rec. 97 Regulation (EU) 2024/1689.
1792 Rec. 99 Regulation (EU) 2024/1689; Schwartmann, R./Keber, T./Zenner, K., KI-VO, Part 2, Chapter 1, para. 16.
1793 Schwartmann, R./Keber, T./Zenner, K., KI-VO, Part 2, Chapter 1, para. 18.
1794 Martini, M./Wendehorst, C., KI-VO, Art. 3 para. 64.
1795 Martini, M./Wendehorst, C., KI-VO, Art. 3 para. 82.

important in this context, however, is the extension in Art. 2(1)(c) of the AIA, according to which providers and operators are also affected if they have their registered office in a third country or are located in a third country, but the output produced by the AI system is used in the Union.[1796] However, the interpretation of the term "use" and the effectiveness of the regulation in view of the hardly possible comprehensive monitoring of internet traffic remain open.[1797]

d) Area exceptions

An important exception to the applicability of the Regulation can be found in Art. 2(12) AIA. Accordingly, the Regulation does not apply to AI systems that are made available under free and open source licences, unless they are placed on the market or put into operation as high-risk AI systems or as an AI system that falls under Art. 5 or 50 of the AIA. This regulation is based, among other things, on the consideration that software and data released under a free and open source licence can contribute to research and innovation on the market and open up significant growth opportunities for the Union economy.[1798] However, AI components only fall under the exception for free and open source AI components under Art. 2(12) of the AIA if they are not made available for a price or otherwise monetised.[1799] However, the provision of AI components via open repositories should not in itself constitute monetisation.[1800] For AI models that are provided under a free and open source licence, the scope exception does not apply, in contrast to AI systems, but Art. 53(2) AIA provides for simplifications with regard to the obligations under Art. 53(1) AIA.

A further exemption under Art. 2(3) of the AIA concerns national security and the military.[1801] According to Art. 2(3) of the AIA, the Regulation does not apply to AI systems if and to the extent that they are placed on the market, put into service or used, with or without modification, solely for military, defence or national security purposes, regardless of the type of entity carrying out these activities. However, an AI system developed and placed on the market for military purposes but temporarily used for civilian purposes falls within the scope of the Regulation.[1802]

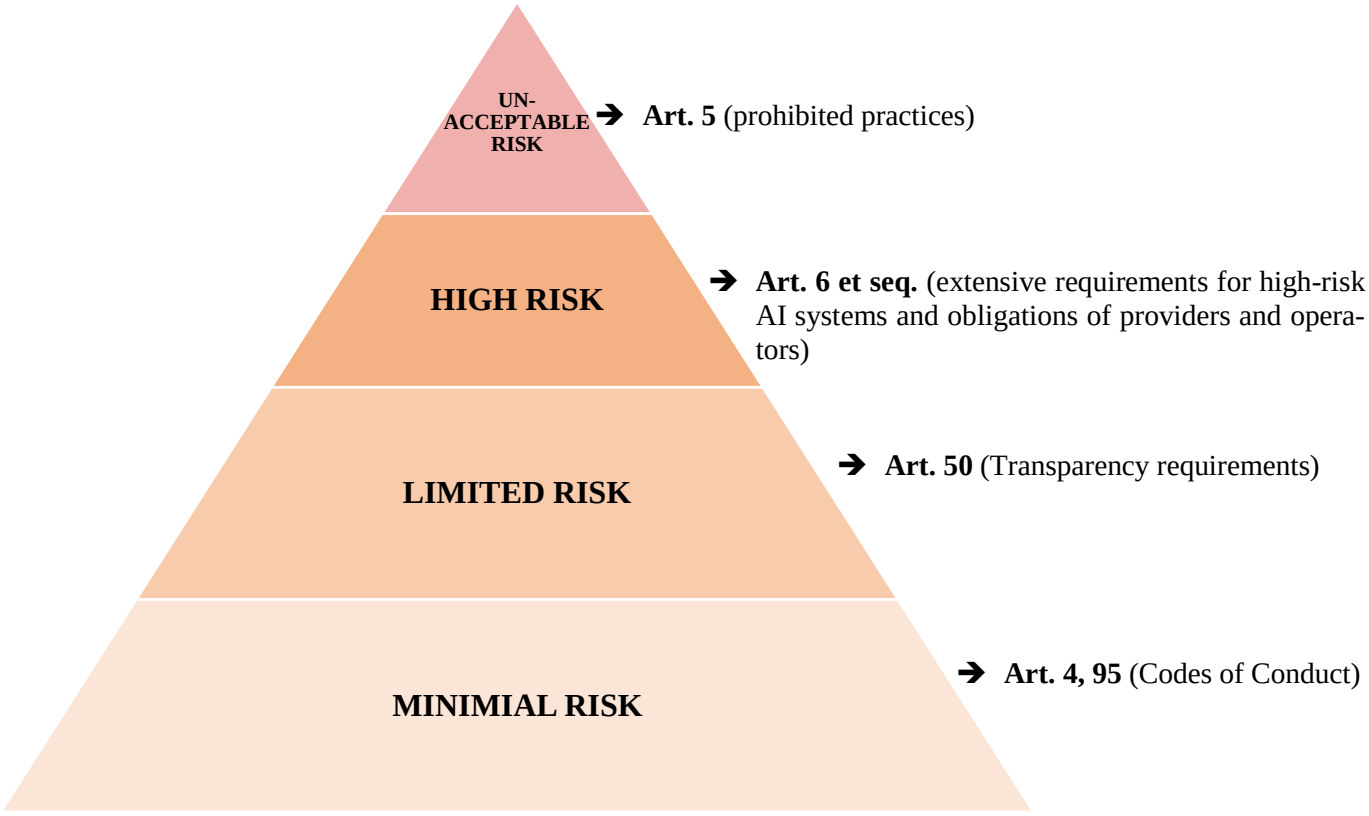
3. Rights and obligations

The AIA is based on **a risk-based approach** to the regulation of artificial intelligence.[1803] Accordingly, the intensity of the respective obligations should vary depending on the degree of risk posed by the respective AI system. To this end, the AIA categorises AI systems into those with unacceptable risks

---

1796 This is intended in particular to prevent circumvention of the Regulation by providers outside the EU, Rec. 22 Regulation (EU) 2024/1689.
1797 Bomhard, D./Siglmüller, J., *RDi* 2024, 46; Möller-Klapperich, J., *NJ* 2024, 337 (339).
1798 Rec.102 Regulation (EU) 2024/1689.
1799 Rec. 103 Regulation (EU) 2024/1689.
1800 Rec. 103 Regulation (EU) 2024/1689; Schwartmann, R./Keber, T./Zenner, K., KI-VO, Part 2, Chapter 1, para. 30 cites internet platforms that act as hosting services, such as GitHub and Hugging Face, as examples of development on open storage.
1801 For background information, see rec. 24 Regulation (EU) 2024/1689.
1802 Schwartmann, R./Keber, T./Zenner, K, KI-VO, Part 2, Chapter 1, para. 41.
1803 Rec. 26 Regulation (EU) 2024/1689; in detail on the risk-based approach Roth-Isigkeit, D., *MMR* 2024, 621.

(Art. 5 AIA), those with high risks (Art. 6–49 AIA) and those AI systems with limited risks (Art. 50 AIA). AI systems that do not fall into any of these three categories are considered to be systems with minimal risk.



Source: Own illustration

Furthermore, general purpose AI models are subject to their own regulations (Art. 51–56 of the AIA). Here, too, a distinction is made between general purpose AI models that are associated with a systemic risk and other general purpose AI models. The tiered regulatory system in the sense of a risk-based approach can also be found in other recent legal acts such as the Digital Services Act[1804] (DSA). [1805]

a) AI literacy, Art. 4 AIA

Irrespective of the risk classification of the respective AI system, general obligations apply to all providers and operators of AI systems, i.e. in particular also for AI systems with minimal risk. According to Art. 4 AIA, all providers and operators must take measures to ensure, to their best extent, the AI

[1804] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), OJ EU L 277, 27.10.2022, p. 1.

[1805] On the graduated system of due diligence obligations for intermediary services Kraul, T./Maamar, N., Das neue Recht der digitalen Dienste, § 4 para. 4.

literacy of the persons who come into contact with the AI systems. The underlying rationale is that those involved in the value creation process should have the necessary knowledge about AI to be able to make informed decisions.[1806] Against the backdrop of rapid technological development in particular, this means that further training should not be underestimated and applies equally to private sector players and public sector body employees.[1807] The aim is also to ensure effectiveness and social responsibility in connection with AI systems.[1808]

b) Prohibited AI practices, Art. 5 AIA

The strictest regulatory effect in the AIA comes from Art. 5 AIA, as certain practices in the field of AI are generally prohibited. This includes certain AI systems that use manipulative techniques or exploit personal weaknesses; AI systems for predicting future criminal offences on the basis of profiling or personality traits and AI systems that create facial recognition databases by reading facial images from the internet or video surveillance systems. However, there are exceptions, particularly in the area of law enforcement, such as for the risk assessment of future criminal offences or for the identification of individuals.
In detail:

Art. 5(1)(a) of the AIA prohibits subliminal influencing by AI systems, i.e. the use of AI systems with the intention of significantly changing the behaviour of individuals by impairing their decision-making ability. Subliminal influence refers to techniques that lie outside a person's awareness and influence their decisions. The commissioning and placing on the market of such AI systems is prohibited.

Art. 5(1)(b) prohibits the placing on the market or commissioning of AI systems that aim to exploit vulnerability. The aim is to prevent such AI systems from altering the behaviour of a vulnerable person or group in a way that causes significant harm to the person themselves or others.

Art. 5(1)(c) prohibits discrimination based on social judgement by AI systems. On the one hand, it mentions the case where the social evaluation leads to a disadvantage for persons outside the context in which the data was originally collected and, on the other hand, the unjustified and disproportionate disadvantaging of persons.

According to Art. 5(1)(d), the use of AI systems to assess risks relating to natural persons is also not permitted. In other words, AI systems with the purpose of predicting the risk of a person committing a criminal offence solely on the basis of the creation of a profile or the assessment of personal characteristics and personality traits. Such an approach harbours a high risk of unequal treatment.[1809]

1806 Rec. 20 Regulation (EU) 2024/1689.
1807 Möller-Klapperich, J., *NJ* 2024, 337, 340.
1808 Martini, M./Wendehorst, C., KI-VO, Art. 4 para. 2.
1809 Schwartmann, R./Keber, T./Zenner, K./Köhler, M., KI-VO, Part 2, Chapter 1, para. 81.

Art. 5(1)(e) also does not permit the untargeted reading of facial images from the internet or from surveillance cameras, which would constitute a major intrusion into the privacy of citizens.[1810]

Art. 5(1)(f) prohibits the use of AI systems to infer the emotions of a natural person in the workplace and in educational institutions. An exception is to be made for the use of the AI system for medical or safety reasons. The reason for the explicit regulation in the workplace and educational institutions is the power imbalance that often exists there.[1811]

The use of AI systems for the biometric categorisation of natural persons is also not permitted under Art. 5(1)(g). For example, it must not be possible to infer or deduce their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. However, the categorisation of biometric data in the area of law enforcement is still permitted.

Finally, Art. 5(1)(h) generally prohibits the use of real-time remote identification systems in publicly accessible areas for law enforcement purposes. This is permitted by way of exception if it is absolutely necessary. This is the case when searching for victims of certain criminal offences or missing persons, averting serious threats or detecting or identifying persons suspected of committing a criminal offence.

However, the impact of Art. 5 AIA on the use of AI will be quite limited. For example, some of the cases regulated in Art. 5 AIA are already prohibited by data protection or criminal procedure provisions.[1812] This partly redundant list of prohibitions can be explained by the desire, driven by legal policy, to take explicit legislative action in these particularly sensitive areas and to pre-empt possible regulatory loopholes.[1813]

c) High-risk AI systems, Art. 6–49 AIA

The centrepiece of the AIA concerns the regulation of **high-risk AI systems**. High-risk AI systems are the most heavily regulated, but nevertheless generally permitted AI systems.[1814] Which AI systems are considered high-risk AI systems is determined by Art. 6, 7 AIA. The specific requirements to be complied with for high-risk AI systems are set out in Art. 8–49 AIA.

aa) Classification of AI systems as high-risk, Art. 6 AIA

The AIA does not contain a legal definition of high-risk systems. Instead, a dynamic system implemented in Art. 6 and Art. 7 AIA was used to categorise AI systems differently.[1815] The Commission must subsequently concretise or adapt these provisions (Art. 6(4)–(8), Art. 7 AIA) and can therefore react to current developments.

1810 Rec. 43 Regulation (EU) 2024/1689; Schwartmann, R./Keber, T./Zenner, K./Pottkämper, E., KI-VO, Part 2, Chapter 1, para. 86; Martini, M./Wendehorst, C., KI-VO, Art. 5, para. 86.
1811 Martini, M./Wendehorst, C., KI-VO, Art. 5 para. 99.
1812 Bomhard, D./Siglmüller, J., *RDi* 2024, 48.
1813 Bomhard, D./Siglmüller, J., *RDi* 2024, 48.
1814 Lachenmann, M., *MMR-Aktuell* 2024, 01359.
1815 Chibanguza, K./Steege, H., *NJW* 2024, 1769 (1772).

(1) Classification in accordance with Art. 6(1) AIA (Annex I)

Art. 6 of the AIA distinguishes between two categories of high-risk systems. An AI system falls into the first category under Art. 6(1) of the AIA if it is used as a safety component for another product or if it is itself a product that is subject to the regulations listed in Annex I. Case groups relevant in practice include toys (Directive 2009/48/EC), medical devices (Regulation (EU) No. 2017/745) and machinery (Directive 2006/42/EC) as well as, in particular, various means of transport such as those used in civil aviation (Regulation No. 300/2008), two- or three-wheeled and four-wheeled vehicles, railways (Directive 2016/797) or recreational craft (Directive 2013/48/EC). Pressure equipment (Directive 2014/68/EU) is also covered, for example.

(2) Classification in accordance with Art. 6(2) AIA (Annex III)

The second category according to Art. 6(2) of the AIA includes an AI system listed in Annex III for areas with a special context relevant to fundamental rights or the common good.[1816] This includes the following fields :

1. Biometrics, insofar as their use is authorised under relevant Union or national law
2. Operation and management of critical infrastructure
3. Education and vocational training
4. Employment, workers' management and access to self-employment
5. Access to and enjoyment of essential private services and essential public services and benefits
6. Law enforcement, insofar as their use is permitted under the relevant Union oder national law
7. Migration, asylum and border control management
8. Administration of justice and democratic processes

For many companies, the area of workers' management (No. 3) will be particularly relevant. This is because many AI systems are likely to be categorised as high-risk systems that are used for the recruitment or selection of natural persons (e.g. to place targeted job advertisements, screen or evaluate applications, etc.) or for assessing a person's performance and assigning tasks.[1817]

(3) Exceptions, Art. 6(3) AIA

However, there are also exceptions to the second category, meaning that AI systems that fall under Annex III do not necessarily have to be considered high-risk AI systems. According to Art. 6(3) of the AIA, AI systems are exempt from being categorised as high-risk AI systems if there is no significant risk to particular legal interests (health, safety, fundamental rights), among other things because it does not influence the outcome of the decision-making process. The exemption applies if the AI system is intended for one of the tasks listed exhaustively in Art. 6(3) AIA: [1818]

[1816] Honer, M./Schöbel, P., *JuS* 2024, 648 (651).

[1817] Förster, A./Gehrmann, M., *SPA* 2024, 113 (115).

[1818] Schwartmann, R./Keber, T./Zenner, K./Hansen, M., KI-VO, 2nd part 1st chapter para. 130; Bronner, *jurisPR-ITR* 13/2024 note 2.

a) Execution of narrowly defined procedural tasks (e.g. rough structuring of data)
b) Improvement of the result of a previously completed human activity (e.g. optimisation of speech)
c) Pattern recognition in previous human decisions (e.g. deviation from certain evaluation patterns)
d) Preparation of a human decision relevant for the purposes of the use cases listed in Annex III (e.g. word processing, translation of texts)

These exemptions are based on the consideration that the AI systems in these areas no longer deserve to be classified as high-risk in view of their specific design. Particularly in the cases of Art. 6(1)(b) and (c) of the AIA, this results from the fact that the human task fulfilment has already been completed and is only subsequently analysed by an AI system. In the case of Article 6(2)(d) of the AIA, on the other hand, the human decision is merely prepared. Frequently used functions such as indexing, searching, text and language processing can be cited as examples[1819], meaning that this exemption could be highly relevant in practice. However, it appears difficult to draw a legally certain distinction between the preparation of a decision and the implementation of a final decision.[1820]

The exemptions are very important in practice due to the far-reaching consequences with regard to the associated obligations.[1821] In general, it should therefore always be checked and also documented whether an AI that should actually be categorised as high-risk AI is exempt from the complex obligations of such systems under Art. 8 et seq. AIA.[1822] If a provider ultimately comes to the conclusion that its AI system listed in Annex III is nevertheless not high-risk, it must document its assessment and submit it to the national supervisory authority upon request, Art. 6(4) of the AIA. However, the danger in self-assessment is that providers may deliberately misjudge their systems in order to avoid the strict requirements.[1823]

Again as a counter-exception, however, an AI system listed in Annex III is considered high-risk under Art. 6(3) of the AIA if it carries out profiling of natural persons, even if one of the aforementioned exceptions applies. Profiling is understood to mean any type of operations

of personal data that the AI system uses to analyse, evaluate or predict personal aspects (Art. 3 No. 52 AIA in conjunction with Art. 4 No. 4 GDPR). Personal aspects include, in particular, work performance, economic situation, health, reliability, behaviour, location or upcoming relocation.

1819 Rec. 53 Regulation (EU) 2024/1689.
1820 Schwartmann, R./Keber, T./Zenner, K./Hansen, M., KI-VO, Part 2, Chapter 1, para. 135.
1821 Bomhard, D./Siglmüller, J., *RDi* 2024, 49; Bronner, *jurisPR-ITR* 13/2024 note 2.
1822 Förster, A./Gehrmann, *SPA* 2024, 113, 115.
1823 Martini, M./Wendehorst, C./Ruschemeier, , KI-VO, Art. 6 para. 90.

bb) Requirements for high-risk AI systems, Art. 8–15 AIA

High-risk AI systems are subject to far-reaching and stringent requirements (Art. 8 et seq. of the AIA), which must be met in particular by providers (Art. 16 AIA) when developing the system. These include the establishment, application and documentation of a risk management system (Art. 9 AIA). This should be a continuous, iterative process that requires regular review and updating. The aim is to improve risk assessment for providers.[1824] There are no specifications in the AIA regarding the exact implementation. However, it should be analysed in particular whether the AI system is being used for its intended purpose.[1825] The steps specified in Art. 9(2) of the AIA must be carried out repeatedly. However, not all risks must be identified, but only those that are known and reasonably foreseeable (Art. 9(2)(a) of the AIA).

The data used to train the high-risk systems must also fulfil certain quality criteria, which are listed in Art. 10 AIA. To ensure this, the data undergoes a so-called data management procedure. Even if the requirements initially only apply to the data sets, they are closely linked to the mathematical model of the AI.[1826] Providers are dependent on the model provider supplying the relevant information.[1827]

Another obligation for providers is the technical documentation. Before placing a high-risk AI system on the market or putting it into service, providers are obliged to prepare technical documentation in such a way that it demonstrates how the high-risk AI system fulfils the requirements of the second section of the AIA. This documentation must be available to the competent national authorities and notified bodies for assessment in a clear and comprehensible form. The technical documentation is also useful for the provider itself. It helps them to implement their risk management system in a verifiable manner.[1828]

Furthermore, providers have recording and logging obligations (Art. 12 AIA). Automatic recording of events is required that are relevant for the identification of situations that may lead to a risk within the meaning of Art. 79(1) of the AIA, that facilitate post-market surveillance in accordance with Art. 72 AIA and that are relevant for the monitoring of high-risk AI systems in accordance with Art. 26(5) AIA.

Providers are also obliged to provide transparency and information to operators (Art. 13 AIA). This is intended to enable operators to fulfil their obligations under the third section of the AIA and to help eliminate concerns regarding the opacity and complexity of high-risk AI systems.[1829] Art. 13(2) of the AIA refers in particular to the appropriate provision of operating instructions, which must contain precise, complete, correct and unambiguous information in a form that is relevant, accessible and comprehensible to operators.

1824 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 5 para. 7.
1825 Schwartmann, R./Keber, T./Zenner, K./Hansen, M., KI-VO, Part 2, Chapter 1, para. 282.
1826 Schwartmann, R./Keber, T./Zenner. K./Köhler, M./Nägele, P., KI-VO, Part 2, Chapter 1, para. 301.
1827 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 5 para. 12.
1828 Schwartmann, R./Keber, T./Zenner, K./Hansen. M., KI-VO, Part 2, Chapter 1, para. 310.
1829 Schwartmann, R./Keber, T/Zenner, K./Köhler, M., KI-VO, Part 2, Chapter 1, para. 329 et seq.; Martini, M./Wendehorst, C., KI-VO, Art. 13 para. 1 et seq.

Human supervision must also be ensured during the period of use to prevent or minimise risks to health, safety or fundamental rights in accordance with Art. 14 AIA. The supervisory measures are based on the risks, the degree of autonomy and the context of use of the high-risk AI system.

Precise regulations on the requirements for the accuracy, robustness and cybersecurity of the system can be found in Art. 15 AIA. Art. 15(4) of the AIA stipulates that high-risk AI systems must be as resilient as possible to errors, malfunctions or inconsistencies that may occur within the system or the environment in which the system is operated. The standardised cybersecurity requirements are particularly relevant from the point of view that high-risk AI systems are exposed to an increased risk of attacks by unauthorised third parties.[1830] The risk of an attack increases with the sensitivity of the system.

In view of the mass of data and the complexity of some systems, it sometimes seems questionable how, for example, data quality requirements under Art. 10(3) of the AIA or effective human supervision under Art. 14 AIA are to be complied with - especially as a conspicuous number of undefined legal terms are used, which weaken the content of the regulations and increase legal uncertainty to the detriment of users.[1831]

cc) Obligations of providers and deployers of high-risk AI systems, Art. 16–22 AIA

If an AI system is a high-risk system, providers and deployers are subject to different levels of obligation. To a lesser extent, other parties who come into contact with the high-risk AI system are also affected by the obligations, such as product manufacturers, importers and distributors. Companies that use high-risk AI systems are subject to a comprehensive catalogue of obligations.

(1) Obligations of providers of high-risk AI systems, Art. 16 AIA

Providers are subject to a particularly extensive catalogue of obligations under Art. 16 of the AIA. Providers are obliged to prove that the requirements of Art. 8 et seq. KI-VO are fulfilled (a) and to provide contact details (b). In addition, the conformity assessment procedure pursuant to Art. 43 KI-VO must be complied with (f), an EU declaration of conformity pursuant to Art. 47 of the AIA must be issued (g), a CE marking pursuant to Art. 48 of the AIA must be affixed (h) and the registration obligations pursuant to Art. 49(1) of the AIA must be fulfilled (i). Reference is also made in particular to compliance with the provisions of Art. 17–20 AIA (c), (d), (e), (j)).

(2) Quality management system, Art. 17 AIA

Art. 17 AIA stipulates that a quality management system must be established and comprehensively documented to ensure compliance with the AIA. Provisions regarding the minimum aspects to be complied with can be found in Art. 17(1) AIA. The extent to which these aspects must be implemented depends on the size of the provider's organisation. At the very least, it must be ensured that the high-risk AI system complies with the provisions of the Regulation, Art. 17(2) AIA. Due to further Union law, Art.

1830 Martini, M./Wendehorst, C., KI-VO, Art. 15 para. 50 et seq.
1831 Bomhard, D./Siglmüller, J., *RDi* 2024, 49.

17(3) of the AIA provides for the possibility of integrating the quality management system into equivalent quality management systems.

(3) Documentation keeping, Art. 18 AIA

Providers are obliged to retain the documentation for ten years from the date of placing on the market or commissioning of the high-risk AI system in accordance with Art. 18 AIA.

(4) Automatically generated logs, corrective actions and duty to inform, Art. 19, 20 AIA

The logs automatically generated by high-risk AI systems pursuant to Art. 12(1) of the AIA must also be retained for at least six months in accordance with Art. 19(1) of the AIA. As soon as the provider has reason to believe that its high-risk AI system does not comply with the AIA, it is also obliged to initiate corrective measures immediately and to inform the traders concerned and, where applicable, the operators, authorised representative and importers (Art. 20 AIA). If a correction is not possible or desired, the provider must withdraw, deactivate or recall the high-risk AI system.

(5) Cooperation with the competent authorities and authorised representatives of providers, Art. 21, 22 AIA

Providers based outside the EU must also appoint an authorised representative who is established within the EU in accordance with Art. 22(1) of the Regulation. This authorised representative assumes further obligations, acts as a contact person for the supervisory authorities and is responsible for implementing the obligations of the AIA, Art. 22(3) AIA.

dd) Obligations of importers of high-risk AI systems, Art. 23 AIA

Importers are obliged to check whether the provider has fulfilled its obligations, whereby the check is limited to formal aspects, Art. 23(1) of the AIA. In the event that there is sufficient suspicion that a high-risk AI system does not comply with the Regulation, the high-risk AI system may not be placed on the market (Art. 2 (2) AIA). Accordingly, the importer may not place the high-risk AI system on the market even if there is a breach of obligations that is not covered by the verification obligation under Art. 23(1) of the AIA.

According to the wording, the duty to inform already applies if the risk is objectively present. However, this would mean that the importer would be more heavily regulated than the supplier.[1832] For this reason, the obligation to provide information must only apply to the importer once he is aware of the risk.[1833]

According to Art. 23(3) of the AIA, the importer is obliged to provide his name, registered trade name and address where he can be contacted in relation to the high-risk AI system. Furthermore, pursuant to Art. 23(6) and (7) of the AIA, he is obliged to cooperate with the national authorities, in particular with regard to measures taken by the authorities to reduce or mitigate the risks posed by high-risk AI systems.

[1832] Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 402.
[1833] Schwartmann, R./Keber. T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 402.

To this end, it must make the technical documentation available to the authorities. Serving the provider or a third party is probably sufficient for this.[1834] The importer's obligation under Art. 23(6) of the AIA is supplementary to that of the provider, with the purpose of closing possible liability gaps.[1835]

ee) Obligations of distributors of high-risk AI systems, Art. 24 AIA

Distributors are also subject to an inspection obligation (Art. 24(1) AIA). This relates to the required CE labelling, the enclosure of a copy of the declaration of conformity as well as operating instructions and compliance with the obligations of providers in accordance with Art. 16(b), (c) AIA and of importers in accordance with Art. 23(3) AIA. In addition, distributors must also comply with information obligations in the same way as providers, deployers and importers (Art. 24(2), (4) AIA).[1836] Distributors are also obliged to co-operate with the competent authorities in the same way as importers. If the high-risk AI system has not yet been placed on the market, the distributor may only make it available to the market as soon as the system has been brought into conformity (Art. 24(2) AIA). If the system has already been placed on the market, the distributor must take the necessary corrective action or withdraw or recall the system. Alternatively, the distributor can also ensure that the supplier, importer or another relevant actor takes appropriate corrective action (Art. 24(4) AIA). As long as the high-risk AI system is under the distributor's responsibility, the distributor must also ensure that the storage or transport conditions do not jeopardise the conformity of the system with the requirements of Chapter III Section 2 in accordance with Art. 24(3) AIA. This makes it clear that the distributor's obligation also applies if the high-risk AI system is part of a physical product into which the high-risk AI system has been integrated.[1837]

In addition, Art. 25 AIA standardises responsibilities along the AI value chain. Accordingly, under certain circumstances, distributors, importers, deployers or other third parties are also subject to the provider obligations under Art. 16 of the AIA as providers. According to Art. 25(1) AIA, this is the case if the high-risk system is placed on the market under its own name or trade mark (a), the high-risk AI system put into operation is significantly modified (b) or the purpose of an AI system not yet classified as high-risk changes in such a way that it becomes a high-risk AI system (c). As a result of the treatment of third parties as providers, the original provider is no longer to be regarded as a provider, Art. 25(2) AIA. However, the initial provider is still obliged to inform and support the new provider in accordance with Art. 25(2) AIA. Art. 25 AIA thus serves to protect both legal certainty and effective law enforcement.[1838]

1834 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 407.
1835 Martini, M./Wendehorst, C./Gössl, S., KI-VO, Art. 23 para. 35.
1836 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, 2nd part 1st chapter para. 411, 414.
1837 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 411.
1838 Martini,M./Wendehorst, C./Gössl, S., KI-VO, Art. 25 para. 2.

ff) Obligations of deployer of high-risk AI systems, Art. 26 AIA

Deployer (Art. 3 No. 4 AIA) of high-risk AI systems have to comply with a significantly reduced catalogue of obligations compared to providers.[1839] This results from Art. 26 AIA and provides for the cardinal obligation in Art. 26(1) AIA to use the AI systems in accordance with the attached operating instructions pursuant to Art. 26(3), (6) AIA, which should be ensured by appropriate technical and organisational measures. In addition, the deployer shall assign human supervision to natural persons who have the necessary competence, training and authorisation and provide them with the necessary support (2).

(1) Purposeful input data, monitoring obligation and retention obligation for automatically generated logs, Art. 26(4)–(6) AIA

Other obligations include ensuring that the input data is suitable and sufficiently representative for the purpose of the system (4). If it is feared that use in accordance with the operating instructions may result in the system posing a risk to health, safety or fundamental rights in accordance with Art. 79(1) AIA, the provider or distributor and the relevant market surveillance authority must be informed and the use of the system suspended (5). The logs automatically generated by their high-risk AI system must also be kept for a period of at least six months appropriate to the purpose of the high-risk AI system, insofar as these logs are subject to their control (6).

(2) Information obligations, Art. 26 (7), (11) AIA

Deployers of the high-risk AI systems listed in Annex III who make decisions concerning natural persons or provide support for such decisions are also obliged to inform natural persons that they are subject to the use of the high-risk AI system (11). Similarly, deployers who, as employers, wish to use a high-risk AI system in the workplace must inform the employee representatives and the employees concerned that they will be subject to the use of this system before it is put into operation or used (7).

(3) Registration, data protection impact assessment and high-risk AI system for subsequent biometric identification, Art. 26 (8), (9), (10) AIA.

According to Art. 26(8) AIA, operators must fulfil the obligation set out in Art. 49(3) AIA to register in the database described in Art. 71 AIA.[1840] However, despite calls in the European Parliament for more extensive obligations, this only applies to deployers that are institutions, bodies, offices or agencies of the Union.[1841] It can therefore be assumed that deployers have an obligation to check whether a system is registered in the EU database before using it.[1842] If this is not the case, they must inform the providers and distributors of this system accordingly.[1843]

1839 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 6 para. 36.
1840 Details can be found in Annex VII Section C.
1841 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 430.
1842 Martini, M./Wendehorst, C./Eisenberger, I., KI-VO, Art. 26 para. 47.
1843 Martini, M./Wendehorst, C./Eisenberger, I., KI-VO, Art. 26 para. 47.

Art. 26(9) of the AIA also stipulates that operators of high-risk AI systems shall also use the information provided in accordance with Art. 13 AIA, where applicable, to fulfil their obligation to carry out a data protection impact assessment in accordance with Art. 35 GDPR or Art. 27 Directive (EU) 2016/680. However, Art. 26(9) AIA does not contain an independent obligation to carry out a data protection impact assessment. Instead, the information is only to be used if necessary, i.e. if a data protection impact assessment is already required under Art. 35 GDPR or Art. 27 of Directive (EU) 2016/680.[1844] However, this should generally be assumed for high-risk AI systems due to an expected high risk to the rights and freedoms of natural persons (Art. 35(1) GDPR).[1845]

In addition, Art. 26(10) AIA contains special rules for operators of a high-risk AI system for retrospective remote biometric identification in the context of investigations into the targeted search of a person suspected of having committed or convicted of a criminal offence. In principle, authorisation must be obtained from a judicial or administrative authority for the use of such a system. The authorisation must be obtained before or when the AI system is used, but at the latest within 48 hours. Any use must also be limited to what is absolutely necessary for the investigation of a specific criminal offence.

(4) Fundamental rights impact assessment, Art. 27 AIA

Operators that are bodies governed by public law or private organisations that provide public services must also carry out a fundamental rights impact assessment prior to the commissioning of a high-risk AI system, Art. 27 AIA. Operators of high-risk AI systems pursuant to Annex III No. 5 (b) and (c) of the AIA, i.e. operators of high-risk AI systems for determining and assessing the creditworthiness of natural persons or for analysing emergency calls from natural persons, are also obliged to do so. These operators must provide an impact assessment that evaluates the impact of the use of the high-risk AI system on fundamental rights, for example in relation to the procedure, the period of use, the categories of natural persons potentially affected, the risk of harm and possible measures. The rights standardised in the Charter of Fundamental Rights serve as the main benchmark for the review.[1846]

d) Transparency obligations for providers and deployers of certain AI systems, Art. 50 AIA

Art. 50 (1)-(4) AIA defines individual AI systems whose providers and deployers are subject **to transparency obligations**. According to Art. 50(6) AIA, the transparency obligations apply cumulatively with other transparency obligations under Union and national law.[1847] Consequently, the information required by the transparency obligations must be provided in a clear, unambiguous and accessible manner at the latest at the time of the first interaction or suspension (Art. 50(5) AIA).

Art. 50(1)–(4) AIA sets out transparency obligations for a total of four specific use cases of AI systems:

1844 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 432.
1845 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 433.
1846 Martini, M./Wendehorst, C./Eisenberger, I., KI-VO, Art. 27 para. 31 et seq.
1847 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 451.

aa) AI systems with direct interaction with natural persons (Art. 50(1) AIA)

In the case of AI systems that are intended for direct interaction with natural persons, providers must ensure that the natural persons concerned are informed about their interaction with AI systems (Art. 50(1) AIA). Unless this is already obvious from the perspective of a reasonably well-informed, attentive and circumspect natural person due to the circumstances and context of use. This is likely to be the case when using GPAI systems such as ChatGPT, Claude, etc., just as if the AI reference were already apparent from the name.[1848] However, such an assessment of obviousness could be stricter with regard to recital 132 AIA if the AI system is also intended to interact with groups that are considered particularly vulnerable due to their age or disability. [1849]

bb) AI systems for the generation of synthetic audio, image, video or text content (Art. 50(2) AIA)

Providers of general-purpose AI systems that generate synthetic audio, image, video or text content must ensure that the outputs of the AI system are machine-readable and recognisable as artificially generated or manipulated (Art. 50(2) of the AIA). In particular, the provider must ensure the interoperability, resilience and reliability of these solutions (Art. 50(2) of the AIA). This is intended to counteract the possible removal of labelling.[1850] Exceptions apply if the AI systems only have a supporting function in standard processing, there is no significant change to the input data or the AI system is legally authorised to fight crime (Art. 50(2) of the AIA). Possible areas for the exceptions would be, for example, AI applications that are embedded to support traditional image processing programmes.[1851]

cc) Emotion recognition systems or systems for biometric categorisation (Art. 50(3) of the AIA)

A special transparency obligation also exists for **emotion recognition systems** or **systems for biometric categorisation** in accordance with Art. 50(3) of the AIA. According to Art. 3 No. 39 of the AIA, an "emotion recognition system" is an AI system that serves the purpose of determining or inferring the emotions or intentions of natural persons on the basis of their biometric data. A "biometric categorisation system", on the other hand, is an AI system that serves the purpose of assigning natural persons to certain categories on the basis of their biometric data, provided that it is an ancillary function of another commercial service and is absolutely necessary for objective technical reasons. The categories may include aspects such as gender, age, hair colour, eye colour, tattoos, personal characteristics, ethnic origin and personal preferences and interests.[1852]

1848 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 460.
1849 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 460.
1850 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 463.
1851 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 9 para. 9.
1852 Rec. 132 Regulation (EU) 2024/1689.

The deployers of such systems are obliged to inform the data subjects about the use of such a system.[1853] Natural persons should therefore know when they are exposed to AI systems that can identify or deduce the feelings or intentions of these persons or assign them to certain categories by processing their biometric data. Emotion recognition systems are used in many different areas, such as in the workplace, in educational institutions, for marketing purposes or in the private or public security sector.[1854]

According to Art. 50(3) AIA, an exception to the transparency obligation is made for AI systems that are legally used for the detection, prevention or investigation of criminal offences, are used for biometric categorisation and emotion recognition in accordance with Union law and have taken appropriate safeguards for the rights and freedoms of third parties.

dd) AI systems for the generation and manipulation of image, sound or video content, deepfakes and texts for public information (Art. 50(4) AIA)

There is a further transparency obligation for operators of AI systems that generate or manipulate image, sound or video content that is a **deepfake** within the meaning of Art. 3 No. 60 AIA (Art. 50(4) AIA). Accordingly, a deepfake is image, sound or video content generated or manipulated by AI that resembles real persons, objects, places, facilities or events and would falsely appear to a person as genuine or truthful.

Deployers must inform users that the content has been artificially created or manipulated. However, this labelling does not lead to a social or legal recognition of deepfakes, but is primarily intended to avoid deceptions about the authenticity of content.[1855]

Who exactly is to be informed about the artificial creation or manipulation is not specified in Art. 50(4) of the AIA. However, it can be assumed that this must be done to all persons potentially affected by the deception, i.e. both the users of the AI system and the general public.[1856]

According to Art. 50(4) of the AIA, such a labelling obligation also applies to operators of an AI system that generates or manipulates text that is published in order to inform the public about matters of public interest.

Exceptionally, this obligation does not apply in both cases if the use is authorised by law for the detection, prevention, investigation or prosecution of criminal offences (Art. 50(4) AIA). The transparency obligation is also to be restricted if the content is part of an obviously artistic, creative, satirical, fictional or analogous work or programme. In such a case, the existence of such generated or manipulated content should be disclosed in a manner that does not impair the presentation or enjoyment of the work, in accordance with Art. 50(4)(1) of the AIA.

[1853] Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T.,, KI-VO, Part 2, Chapter 1, para. 466.
[1854] Martini, M./Wendehorst, C., KI-VO, Art. 50 para. 75.
[1855] Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 470.
[1856] Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 471.

An exception to the transparency obligation also exists for operators of AI systems that generate or manipulate texts if the content generated by AI has undergone a process of human review or editorial control and if a natural or legal person bears editorial responsibility for the publication of the content (Art. 50(4) AIA).

The aforementioned obligations will be of practical relevance in particular for companies that use AI systems in the end customer sector.[1857]

e) AI models with a general purpose, Art. 51–56 AIA

Chapter V of the Regulation contains special provisions for general purpose AI models. These systems are also referred to as **general purpose AI (GPAI**) or **basic models**. Generative AI models are a typical example of this, as they enable the flexible generation of content - for example in the form of text, audio, image or video content, which can cover a wide range of different tasks.[1858] These systems are currently based in particular on large language ***models***. The chatbot *ChatGPT* from the company *OpenAI* seems almost omnipresent in this context.[1859]

This category to be regulated was only introduced in the legislative process by the European Parliament's draft[1860] in 2022.[1861] Due to their general purpose, base models are usually not subject to any of the other regulations, as no specific application scenario can be identified.

aa) Classification, Art. 51 AIA

The Regulation distinguishes between general purpose AI models and **general purpose** AI models **with systemic risk** with regard to the obligations for providers. According to Art. 3 No. 66 of the AIA, a general-purpose AI model is an AI model - including cases where such an AI model is trained with a large amount of data under extensive self-monitoring - that has significant general usability and is capable of competently performing a wide range of different tasks, regardless of how it is placed on the market, and that can be integrated into a variety of downstream systems or applications, with the exception of AI models that are used for research and development activities or prototyping before being placed on the market. The categorisation of the model as posing a systemic risk is based on Art. 51 AIA. Accordingly, there are two ways in which an AI model with a general purpose can be categorised as posing a systemic risk. On the one hand, it is categorised as such if it has capabilities with a high degree of effectiveness that are assessed using appropriate technical tools and methods, including indicators and benchmarks (Art. 51(1)(a) AIA). What is meant by a high level of efficiency is explained in Art.

1857 Ashkar, D./Schröder, C., *BB* 2024, 779.
1858 Rec. 99 Regulation (EU) 2024/1689.
1859 von Welser, M., GRUR-Prax 2024, 485 para. 7.
1860 European Parliament, Amendments of the European Parliament of 14 June 2023 to the Act on Artificial Intelligence and amending certain Union acts (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_DE.html.
1861 Schwartmann, R./Keber, T./Zenner, K./Hansen, M., KI-VO, Part 2, Chapter 1, para. 489 et seq.

51(2) AIA: this is assumed to be the case if the cumulative amount of calculations used for training, measured in floating point operations (FLOPs), is more than 10^{25} .[1862]

Classification as a systemic risk model can also be made by a decision of the Commission (Art. 51(1)(b) AIA). Accordingly, the Commission may, with reference to the criteria set out in Annex XIII, categorise an AI model with a general purpose of use as having a high degree of effectiveness on an individual basis, either ex officio or following a warning from the scientific panel. The categorisation determines whether providers are subject to particularly strict obligations to safeguard public interests.[1863]

The provider is obliged to notify the Commission immediately as soon as an AI model with a general purpose fulfils the condition of systemic risk (Art. 52 AIA).

bb) Obligations for providers of general purpose AI models , Art. 53 AIA

According to Art. 53 AIA, providers of general purpose AI models are obliged, among other things, to create and maintain up-to-date technical documentation for their model. The documentation must include the training and testing procedures and the results of the assessment, but at least all the information listed in Annex XI. Information required in Annex XI Section 1 No. 1 includes a general description of the AI model, including the tasks the model is intended to fulfil and the type and nature of the AI systems into which it can be integrated (Annex XI Section 1 No. 1 (a) and the applicable rules of acceptable use (Annex XI Section 1 No. 1(b). Detailed descriptions of the elements of the model and relevant information on the development process, such as the technical means required for the integration of the general purpose AI model in AI systems, are also required (Annex XI Section 1 No. 2 (a)).

Copyright regulations are also a key factor here. The particular importance arises from the fact that the AI models are trained with a huge amount of data, including works that may be protected by copyright.[1864] The AIA stipulates that a strategy for compliance with Union copyright law and related rights must be put in place (Art. 53(1)(c) AIA). During the legislative process, it was long disputed whether there should be independent provisions in the regulation in this regard or whether reference should merely be made to copyright law, with the latter being decided in favour.[1865] The strategy required by Art. 53 AIA also pursues the goal of using state-of-the-art technologies to ensure that a reservation of rights asserted in accordance with Art. 4(3) AIA of the DSM Directive[1866] is upheld.[1867] In this context, the obligation of providers under Art. 53(1)(d) AIA also becomes significant, according to which providers must also prepare and publish a sufficiently detailed summary of the content used for the training

1862 Schwartmann, R./Keber, T./Zenner, K./Kremer, S./Haar, T., KI-VO, Part 2, Chapter 1, para. 494.
1863 Martini, M./Wendehorst, C./Berstein, C./Schmitt, R., KI-VO, Art. 51 para. 3.
1864 For a more detailed introduction and categorisation in copyright law, see *Wendt/Wendt*, Das neue Recht der Künstlichen Intelligenz, § 10 para. 34.
1865 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 10 para. 39.
1866 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, p. 92.
1867 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 10 para. 37.

of the general purpose AI model in accordance with a template provided by the Office for Artificial Intelligence.

Furthermore, providers established in third countries are obliged to appoint an authorised representative established in the Union in writing before placing a general purpose AI model on the Union smart market (Art. 54(1) AIA). This authorised representative must then be enabled to perform the tasks specified in the mandate received from the provider (Art. 54(2) AIA). In particular, the authorised representative must provide the Artificial Intelligence Office with a copy of the mandate upon request in accordance with Art. 54(3) AIA. The mandate authorises the authorised representative to perform at least the tasks listed in Art. 54(3)(a)–(d) of the AIA (Art. 54(3) AIA).

cc) Obligations for providers of general purpose AI models with systemic risk , Art. 55 AIA

Providers of general purpose AI models with systemic risk must fulfil four additional obligations (Art. 55 AIA). Firstly, providers must carry out a model assessment using standardised protocols and tools that correspond to the state of the art, which also includes carrying out and documenting attack tests on the model (a). This is intended to recognise and reduce systemic risks. In addition, potential systemic risks must be assessed and mitigated (b).[1868] Furthermore, there is an obligation to record and document serious incidents and inform the competent national authority (c). Finally, an appropriate level of cyber-security must also be ensured for the general purpose AI models with systemic risk and the physical infrastructure of the model (d).

dd) Practical guidelines, Art. 56 AIA

In order to contribute to the proper application of the Regulation, practical guides will be developed at Union level (Art. 56 AIA). This is facilitated and promoted by the Office for Artificial Intelligence (Art. 56(1) AIA). The practical guidelines apply to the obligations of providers of AI models with a general purpose, both with and without systemic risk, and are intended to provide concrete guidance on how the abstract obligations can be fulfilled in a legally compliant manner.[1869] In this respect, Art. 56 of the AIA does not lay down any binding obligations for providers, but only provides a framework for voluntary regulations.[1870] In particular, the practical guidelines should at least cover the obligations set out in Art: 53 and 55 AIA (Art. 56(2) of the AIA).

The regulations on general purpose AI models are expected to enter into force in July 2025 in accordance with Art. 113(b) AIA. Accordingly, the practical guidelines in accordance with Art. 56(9) AIA should already be finalised in April 2025. However, it will hardly be possible to achieve this in time due to the

---

1868 This obligation already largely corresponds to the obligation under (a), *Schwartmann/Keber/Zenner/Hansen*, KI-VO, 2nd part 1st chapter para. 497.

1869 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 10 para. 47.

1870 Martini, M./Wendehorst, C./Berstein, C./Schmitt, R., KI-VO, Art. 56 para. 1.

lack of a sufficient EU budget and the fact that the AI Office in Brussels has not yet been finalised.[1871] It is unclear what the consequences will be if the practical guidelines are not available in time.[1872]

The standardisation organisations CEN and CENELEC are also currently preparing industry standards, which will ultimately be published as harmonised European standards in collaboration with the EU Commission.[1873]

ee) Standards, conformity assessment, certificates, registration , Art. 40–49 AIA

The implementation of conformity assessment procedures before the AI system is placed on the market or commissioned is a central component of the regulation's risk-based regulatory approach. The conformity assessment procedure in accordance with Art. 43 AIA, during which compliance with the legal requirements is checked, is mandatory for the provider (Art. 16(f) of the AIA). Once the procedure has been successfully completed, providers are obliged to affix a physical or digital **CE marking** to ensure that the AI system is fit for the internal market in practice (Art. 48 AIA) and to issue an EU declaration of conformity (Art. 47 AIA). The background to this is, on the one hand, the legislator's hope that CE markings will have a positive effect on Europe as an AI location if they can establish themselves as an international AI seal of quality.[1874] On the other hand, the conformity assessment procedure can contribute to the minimisation of AI-specific risks as a precautionary measure and thus to increased safety in legal transactions.[1875]

The **conformity assessment** itself is defined in Art. 3(20) AIA as a procedure to demonstrate whether a high-risk AI system has fulfilled the requirements set out in Art. 8 et seq. AIA. The Regulation offers two different conformity assessment procedures: the internal conformity assessment procedure in accordance with Annex VI or an external conformity assessment procedure in accordance with Annex VII (Art. 43(1)(a), (b) AIA).

In an internal conformity assessment, the provider uses the technical documentation to check whether the AI system meets the requirements of a high-risk AI system, whether the quality management system meets the requirements of the AIA and whether the design and development process of the AI system and its post-market surveillance comply with the technical documentation.[1876]

While in the internal procedure the provider itself verifies compliance with the material requirements of the Regulation, this task is performed by a notified body in the external procedure. The requirements for classification as a notified body are based on Section 4. They are conformity assessment bodies and are inspected by government bodies.[1877] The notification procedure is defined in Art. 28–39 of the AIA.

1871 Schwartmann, R./Keber, T/Zenner, K./Hansen, M., KI-VO, Part 2, Chapter 1, para. 499.
1872 Schwartmann, R./Keber, T./Zenner, K./Hansen, M., KI-VO, Part 2, Chapter 1, para. 499.
1873 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 10 para. 42.
1874 Gerdemann, S., *NJW* 2024, 2209, 2210.
1875 Gerdemann, S., *NJW* 2024, 2209, 2210.
1876 Voigt, P./Hullen, N., Handbook AI Regulation, Chapter 6.1.2.
1877 Voigt, P./Hullen, N., Handbook AI Regulation, Chapter 6.1.3.1.

In the case of an external conformity assessment procedure, the supplier must first submit an application for review of the quality management system and the technical documentation (Annex VII No. 3.1, No. 4.2). This is followed by an assessment by the notified body based on the content specified by the provider in the applications. The notified body determines whether the requirements of the AIA and the regulations on high-risk AI systems have been complied with.

4. Notifying authorities and notified bodies, Art. 28–39 AIA

For the purposes of this Regulation, each Member State must establish or designate at least one **notifying authority** and at least one market surveillance authority as national competent authorities (Art. 70 CPR). The notifying authority is then responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their surveillance (Art. 28(1) and Art. 3 No. 19 CI Regulation). In order for a body to be notified, it must fulfil the requirements set out in Art. 31 of the CIE Regulation – for example with regard to independence and organisational structure.

The certificate of conformity is only issued by the notifying authority for a limited period of time (Art. 44(2) AIA). Certificates for AI systems covered by Annex I are valid for up to five years and for AI systems covered by Annex III for up to four years. It is possible to extend the validity of the certificate by up to four or five years respectively (Art. 44(2) AIA). The certificate can be suspended, revoked or restricted at any time if it is determined that an AI system no longer fulfils the requirements and compliance is not restored by the provider through suitable corrective measures within a period set by the notified body (Art. 44(3) AIA).

It is still unclear which authority in Germany will be responsible for notifying the relevant bodies, although it is widely expected that the Bundesnetzagentur (BnetzA) will take on this role.[1878] Similar to the existing practice in product safety law, it would also make sense for the authority responsible for notification to rely on a preliminary inspection by the German Accreditation Body (DAkkS).[1879]

5. Governance

The AIA should create a governance framework that enables both the coordination and support of the application of this Regulation at national level as well as capacity building at Union level and the integration of stakeholders in the field of AI.[1880] The new governance framework is composed of the EU Commission and new bodies at EU level as well as competent authorities at national level yet to be determined.[1881] Of particular practical relevance are the Office for Artificial Intelligence, the AI Panel and the national authority for market surveillance. The corresponding provisions can be found in Art. 64 et seq. AIA.

1878 Gerdemann, S., *NJW* 2024, 2209, 2211.
1879 Gerdemann, S., *NJW* 2024, 2209, 2211.
1880 Rec. 148 Regulation (EU) 2024/1689.
1881 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 12 para. 1.

a) Office for Artificial Intelligence (AI Office), Art. 64 AIA

The Artificial Intelligence Office (**AI Office**) and the European Artificial Intelligence **Board (AI Board**) are intended to bundle advisory competences in the field of artificial intelligence.[1882] The provisions relating to the AI Office can be found in Art. 64 et seq. AIA. The AI Office is intended to ensure the proper implementation of the AIA, giving it a central role in the AI supervisory system.[1883] In organisational terms, the AI Office is located within the Commission. According to the Commission, it consists of five units and two additional advisors, one senior scientific advisor and one for international affairs.[1884] The AI Office has particular powers as a market surveillance authority for general-purpose AI models.[1885] In this regard, the development of practical guidelines is to be promoted and facilitated (Art. 56 AIA). In order to be able to exercise these powers effectively, the AI Office is authorised to carry out monitoring measures in accordance with Art. 89 AIA. Downstream providers also have the right to report alleged infringements by providers of AI models to the AI Office (Art. 89 (2) AIA).

b) AI Board (AI Board), Art. 65, 66 AIA

In addition to the AI Office, the AI **Board** is to be an additional body to assist with the implementation of the AIA.[1886] As the European Committee on Artificial Intelligence, the AI Board is to be made up of one representative from each member state (Art. 65(2) AIA). The tasks of the AI Board are set out in Art. 66 AIA: The AI Office is given central powers with regard to coordinating and advising national authorities and the Commission (Art. 66(a), (b), (c), (e), (f) AIA), harmonising administrative practice (Art. 66(d) AIA) and developing common criteria with regard to the concepts provided for in the Regulation (Art. 66(g) AIA). The AI Board should also participate in cooperation with the authorities of third countries and other international organisations (Art. 66(i) AIA). The AI Board therefore acts primarily by issuing opinions and reports.[1887] However, it has no binding decision-making powers in individual cases.[1888]

At national level, one notifying authority and at least one market surveillance authority are to be designated for each member state (Art. 70 AIA). The national bodies are to play a key role in the application and enforcement of the AIA.[1889] The tasks of the notifying authorities are mainly derived from Art. 30 et seqq. of the Regulation, which govern notifications for conformity assessment bodies in particular.

1882 Bomhard, D./Siglmüller, J., *RDi* 2024, 52.
1883 Bomhard, D./Siglmüller, J, *RDi* 2024, 52; Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, Section 12 para. 10.
1884 https://digital-strategy.ec.europa.eu/en/policies/ai-office (last accessed on: 1 November 2024).
1885 Bomhard, D./Siglmüller, J, RDi 2024, 52.
1886 Rec. 20 Regulation (EU) 2024/1689.
1887 Martini, M./Wendehorst, C./Roth-Isigkeit, D., KI-VO, Art. 64 para. 4.
1888 Martini, M./Wendehorst, C./Roth-Isigkeit, D., KI-VO, Art. 64 para. 4.
1889 Rec. 153 Regulation (EU) 2024/1689.

c) Market surveillance authority, Art. 3 No. 26 AIA

According to Art. 3 No. 26 of the AIA, the national market surveillance authority is the national authority that carries out the activities and takes the measures prescribed in the Market Surveillance Regulation[1890]. In particular, they are to monitor the enforcement of the high-risk AIAs.[1891] The key tasks of the market surveillance authorities include the following: [1892]

- the receipt and processing of reports of serious incidents (Art. 73(8) AIA in conjunction with Art. 19 Regulation (EU) 2019/1020);
- the market surveillance and control of AI systems (Art. 74 AIA in conjunction with Regulation (EU) 2019/1020);
- administrative assistance and market surveillance and control of GPAI systems (Art. 75 AIA in conjunction with Regulation (EU) 2019/1020);
- the supervision of tests under real conditions (Art. 76 AIA);
- the implementation of procedures at national level for dealing with AI systems that pose a risk (Art. 79 AIA in conjunction with Art. 3 No. 19 and Art. 18 Regulation (EU) 2019/1020);
- the implementation of procedures for dealing with AI systems that are not classified as high-risk by the provider in accordance with Annex III (Art. 80 AIA in conjunction with Art. 11 Regulation (EU) 2019/1020);
- the implementation of the safeguard clause procedure (Art. 81 AIA in conjunction with Art. 11 Regulation (EU) 1025/2012);
- the identification of compliant AI systems that nevertheless harbour a risk (Art. 82 AIA);
- the determination of formal non-compliance (Art. 83 AIA).

The central powers of the market surveillance authority are therefore primarily those for investigation and supervisory measures.

The starting standard for investigative powers is Art. 74 AIA. According to Art. 74(1) AIA, the FMIO applies to AI systems. This obliges the member states to transmission the corresponding powers to the authorities in accordance with national law (Art. 14(1) FMIO). In Germany, this has been implemented with the Market Surveillance Act[1893] (MüG), which in turn refers to the powers under Art. 14(4) and (5) of the FMD Regulation in § 7(1) MüG. In particular, the national market surveillance authority can request documents and information on technical aspects of the AI system or carry out unannounced on-site inspections (§ 14(4)(a), (d) of the FMD). In addition, market surveillance authorities are granted

1890 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ 2019 L 169/1.

1891 Lachenmann, M., *MMR-Aktuell* 2024, 01359; Ashkar, D/Schröder, C, *BB 2024*, 775.

1892 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 12 para. 57.

1893 Act on Market Surveillance and Ensuring the Conformity of Products (Market Surveillance Act - MüG of 9 June 2021, Federal Law Gazette 2021 I p. 1723.

access to the source code of the high-risk AI system upon reasoned request and under certain conditions in accordance with Art. 74(13) AIA. However, companies' business secrets that may be affected must be handled sensitively.[1894]

Supervisory measures in the event of breaches of the AIA are based in particular on the general clause in Art. 79(2) AIA. Accordingly, in the event that the AI system does not fulfil the requirements and obligations of the Regulation, the market surveillance authority may request the relevant actor to take all corrective measures that are appropriate to bring the AI system into conformity. The authority may also require the actor to withdraw the AI-system from the market or to recall it within a period that the market surveillance authority may specify, in any case within less than 15 working days, or in accordance with the relevant Union harmonisation legislation (Art. 79(2) AIA).

6. Sanctions

Art. 99 AIA provides for a catalogue of fines to sanction violations of the AIA. The addressees of the sanctions and enforcement measures can be suppliers, importers, authorised representatives, distributors, operators and notifying bodies.[1895] The amount of the fines depends on the respective violation of the AIA:

a) Fines

aa) Violation of prohibited practices in the AI sector, Art. 99(3) AIA

Failure to comply with the prohibition in Art. 5 of the AIA may result in fines **of up to EUR 35,000,000** or, in the case of companies, **up to 7% of the total worldwide annual turnover of the previous financial year**, whichever is the greater (Art. 99(3) AIA).

However, if there is a breach of obligations under the AIA outside of Art. 5 AIA, fines **of up to EUR 15,000,000** may be imposed in accordance with Art. 99(4) AIA and, in the case of companies, **up to 3% of the worldwide annual turnover of the previous financial year**, whichever is the greater.

If an actor passes on false information to the competent authority, fines of EUR 7,500,000 or, in the case of companies, up to 1% of the total global annual turnover of the previous financial year may be imposed (Art. 99(5) AIA).

For SMEs, the lower of the sums or percentages specified in Art. 99(3)–(5) TFEU applies, Art. 99(6) TFEU. According to the interpretation of Art. 101 and 102 TFEU, the worldwide annual turnover of companies is presumably calculated on the basis of the turnover of the parent company.[1896]

The catalogue of fines itself already has a deterrent effect due to its high penalties. To further ensure the proper enforcement of the AIA, Art. 99(1) of the AIA also authorises the competent national authorities to impose further sanctions and enforcement measures. The sanctions provided for by the Member States

1894 Schwartmann, R./Keber, T./Zenner, K./Hansen, M., KI-VO, Part 3, Chapter 1, para. 35.
1895 Schwartmann, R./Keber, T./Zenner, K./Köhler, M., KI-VO, Part 3, Chapter 3, para. 4.
1896 Schwartmann, R./Keber, T./Zenner, K./Köhler, M., KI-VO, Part 3, Chapter 3, para. 9.

must be effective, proportionate and dissuasive (Art. 99(1) AIA). In addition, the interests of SMEs, in particular their economic survival, should be taken into account.

b) Further liability risks

The AIA does not include any provisions on civil liability. This will be governed by a dual liability framework[1897], namely the Product Liability Directive and the Directive on the Adaptation to Artificial Intelligence of the rules on non-contractual civil liability (AI Liability Directive)[1898] . These are intended to make liability risks easier to calculate and insure.[1899] The directives simplify the rules on presentation and burden of proof for injured parties and also the presumption in favour of manufacturers and providers of AI systems.[1900] The background to the efforts to modify the liability of manufacturers and providers of AI systems is the peculiarities of these systems: characteristics such as complexity, autonomy and opacity (black box effect) pose a number of difficulties for liability cases.[1901]

For example, weaknesses in product liability law in the German Product Liability Act (ProdHaftG) - which is not originally applicable to software (§ 2 ProdHaftG) - are that it does not recognise a product monitoring obligation, which is particularly important for self-learning AI systems.[1902] In contrast, the Commission's draft[1903] on the new Product Liability Directive defines software as a product and takes into account errors in products that continue to learn and places "cybersecurity requirements" on the product.[1904]

Against the background of the peculiarities of AI systems, similar difficulties also exist for tortious liability. It is often almost impossible for the injured party to fulfil the burden of presentation and proof with regard to the breach of the duty of care and the causality giving rise to liability.[1905] The draft AI Liability Directive (AILD-E) therefore provides for similar measures to the revised Product Liability Directive and in particular contains evidence-related provisions. For example, the claimant is entitled to disclosure of certain evidence in the case of high-risk AI systems.[1906] If the defendant fails to comply with the court's request, a rebuttable presumption of a breach of a duty of care is provided for.[1907] In

1897 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 14 para. 1.
1898 EU Commission, Proposal for a Directive of the European Parliament and of the Council adapting the rules on non-contractual civil liability to artificial intelligence (AI Liability Directive) of 28 Sep. 2022, COM(2022) 496 final.
1899 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 14 para. 1.
1900 Lachenmann, M./Meyer, J., *MMR-Aktuell* 2023, 457000.
1901 Schwartmann, R./Keber, T./Zenner, K./Kessen, M., KI-VO, Part 3, Chapter 2, para. 17; Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 14 para. 5.
1902 Schwartmann, R./Keber, T./Zenner, K./Köhler, M., KI-VO, Part 3, Chapter 2, para. 19.
1903 Proposal for a Directive of the European Parliament and of the Council of 28 September 2022 on liability for defective products - COM(2022) 495 final.
1904 Schwartmann, R /Keber, T./Zenner, K./Köhler, M., KI-VO, Part 3, Chapter 2, para. 20.
1905 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 14 para. 8.
1906 Art. 3(1) AILD-E.
1907 Art. 3(5) AILD-E.

addition, under certain conditions, a causal link between the defendant's fault and the result produced by the AI system or the fact that the AI system did not produce a result is presumed.[1908]

Both directives therefore serve to take account of the special technical features of AI, in particular through modified rules on presentation and burden of proof, and to neutralise the previous weaknesses of the liability regulations.

c) Legal remedies

In addition to other administrative or judicial rights, there is a right under Art. 85(1) AIA to lodge a complaint with the competent market surveillance authority if there is reason to believe that the provisions of the AIA have been violated. This right can be exercised by any natural or legal person.

According to Art. 86 AIA, every person affected by an AI-based decision has the right to receive clear and meaningful explanations from the operator regarding the role of the AI system in the decision-making process and the most important elements of the decision taken.

There are no expressly regulated appeal procedures with regard to a failed or revoked notification.[1909] Nevertheless, according to Art. 99(10) AIA, corresponding procedural guarantees and judicial remedies against official powers under the AIA are generally guaranteed. All rights and remedies remain unaffected for consumers and other persons who may be adversely affected by AI systems with regard to possible compensation and are fully applicable.[1910]

7. Summary and implications for practice

a) General criticism of the regulatory concept

Since the plans for the AIA were announced, there have been discussions about the general need to regulate AI systems and whether the current time is right for large-scale regulation.[1911] Supporters, including the Commission in particular, emphasise the EU's pioneering legal position through what is now the first comprehensive AI legislation.[1912] It is hoped that the AIA will create the so-called **Brussels effect**[1913] , which could have a knock-on effect on the AIA of other non-EU member states.[1914] Above all, a rapid regulatory response is necessary due to the rapid technical developments and the dangers, some of which are still barely foreseeable.[1915] Well-known figures from the AI industry have also called

---

1908 Art. 4(1) AILD-E.
1909 Wendt, J./Wendt, D., Das neue Recht der Künstlichen Intelligenz, § 12 para. 62.
1910 Rec. 9 Regulation (EU) 2024/1689.
1911 Bomhard, D./Siglmüller, J., *RDi* 2024, 54 et seq.
1912 https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.
1913 Steege, H./Chibanguza, K., Metaverse, Section 8 para. 7; *Chibanguza/Steege*, *NJW* 2024, 1775; https://rsw.beck.de/zeitschriften/rdi/editorial/2023/08/29/der-br%C3%BCssel-effekt (last accessed on: 1 November 2024).
1914 Becker, D./Feuerstack, D., *KIR 2024*, 64.
1915 Steege, H./Chibanguza, K., Metaverse, § 8 para. 7.

for greater regulation of AI and moratoria on development to allow time to identify dangers and counteract irreversible risks.[1916] Early regulation and a standardised legal framework could also ensure legal certainty and promote a single market, which could ultimately benefit economic development and innovation.[1917]

At the same time, many voices were raised that considered the regulation to be premature.[1918] It is feared that the AIA will create new legal uncertainties through excessive and difficult-to-understand regulation and could therefore significantly inhibit the EU's innovative strength in the area of AI application and development.[1919] Further regulation is also criticised as an obstacle to investment and innovation because the European AI economy appears to be lagging behind the USA and the People's Republic of China.[1920] The AIA would be problematic for young European AI companies in particular, as they do not yet have the necessary financial resources for legal advice or the integration of the prescribed procedures.[1921] On the other hand, more established companies from non-EU member states would have a competitive advantage and the opportunity to further expand their already favourable market position.[1922] There would be a risk of oligopolisation of the market.[1923] In this regard, comparisons are regularly drawn with previous regulations, in particular the GDPR.[1924] Here, too, it is often criticised that American big tech companies in particular (especially '*Alphabet'*, '*Amazon'*, '*Apple'*, '*Meta Platforms'* and '*Microsoft'*) ultimately benefited from the regulation for similar reasons.[1925] Even Gabriele Mazzini, who was formerly responsible for drafting the AIA within the Commission, expressed such concerns about European start-ups being at a disadvantage.[1926]

b) In detail

Aside from the general criticism of the regulatory concept itself, individual provisions of the AIA have been criticised in the specialist literature since the publication of the Commission's first draft. In some cases, the AIA's definition of AI systems under Art. 3 No. 1 AIA has been criticised as being too broad, meaning that it could also cover technologies that are more like conventional software and not artificial intelligence.[1927] Accordingly, an AI system is, among other things, a machine-supported system that is designed for a varying degree of autonomy. Autonomy should mean that the AI system can act independently of human intervention to a certain extent and is able to "work without human intervention".[1928]

1916 https://futureoflife.org/open-letter/pause-giant-ai-experiments/.
1917 Rec. 1, 2, 8, 25 Regulation (EU) 2024/1689.
1918 Bomhard, D./Siglmüller, J., *RDi* 2024, 54 et seq.
1919 Bomhard, D./Siglmüller, J., *RDi* 2024, 54.
1920 Hacker, P./Berz, H., *ZRP* 2023, 226 et seq.
1921 Bomhard, D./Siglmüller, J., *RDi* 2024, 54; Hacker, P/Berz, A, *ZRP 2023*, 227.
1922 Becker, D./Feuerstack, D., *KIR* 2024, 69, Hacker, P/Berz, A, *ZRP 2023*, 227.
1923 Hacker, P./Berz, H., *ZRP* 2023, 227.
1924 Hacker, P./Berz, H., *ZRP* 2023, 227.
1925 Geradin, D./Karanikioti, T./Katsifis, D., 17 Eur. Compet. J. 2021, 47.
1926 https://www.bloomberg.com/opinion/articles/2024-08-01/europe-s-new-ai-rules-have-us-tech-in-mind-they-might-miss?leadSource=uverify%20wall.
1927 Hacker, P./Berz, H., *ZRP* 2023, 226, 227.
1928 Rec. 12 Regulation (EU) 2024/1689.

It is obvious that quite conventional everyday devices can also achieve this level of autonomy. However, the criticism levelled against it can be mitigated by looking at the definition in Art. 3 No. 1 AIA as a whole. Finally, the AI system must also be adaptable and derive from inputs for explicit or implicit goals how outputs (e.g. predictions, content, recommendations, decisions) are created that can influence the physical or virtual environment.

aa) Impending legal uncertainty and lack of clarity regarding the purpose of the law

The criticism of the overly broad definition of AI systems is accompanied by the resulting legal uncertainty. But it is not only Art. 3(1) AIA that is criticised. Generally speaking, the regulation is sometimes unclear.[1929] The often imprecise details of the AIA need to be further concretised by the Commission. However, the main problem here is that the AIA and its obligations are to be implemented before the guidelines are finalised by the Commission.[1930] Legal uncertainty is also increased by the parallel entry into force of other new regulations, such as the Data Act or the Cyber Resilience Act, which are not harmonised with each other.[1931]

bb) Diffuse regulatory purposes

Another point of criticism is that the legislative process has made the purpose of the law unclear by overloading it with secondary issues such as copyright and environmental protection.[1932] The primary objective is to promote the introduction of human-centred and trustworthy AI.[1933] In the legislative process, however, many points were added that have nothing to do with this. This has led to a "watering down"[1934] of the actual objective. The implementation of high-risk AI systems is also inconsistent.[1935] For example, the AIA categorises some harmless AI models as high-risk AI systems and regulates them more strictly than those that are actually dangerous.[1936]

It is also uncertain whether the goal of protecting fundamental rights through product safety regulation can be achieved at all due to the different understanding of risk between the protection of fundamental rights and product safety.[1937]

Ultimately, only the actual implementation of the AIA will show to what extent these points of criticism are justified.

1929 Bomhard, D./Siglmüller, J., *RDi* 2024, 54.
1930 Bomhard, D./Siglmüller, J., *RDi* 2024, 54.
1931 Bomhard, D./Siglmüller, J., *RDi* 2024, 54.
1932 Bomhard, D/Siglmüller, *RDi* 2024, 53.
1933 Rec. 1 Regulation (EU) 2024/1689.
1934 Bomhard, D./Siglmüller, J., *RDi* 2024, 53.
1935 Bomhard, D./Siglmüller, J., *RDi* 2024, 53; *Hacker*, GRUR 2023, 289 et seq.
1936 Bomhard, D./Siglmüller, J., *RDi* 2024, 53; *Hacker*, GRUR 2023, 289 et seq.
1937 Martini, M./Wendehorst, C./Ruschemeier, H., KI-VO, Art. 6 para. 101, 105.

c) Practical implications

For companies that act as providers or deployers of AI systems, this results in a complex range of obligations with technical and organisational requirements, various restrictions and information obligations. However, all of these regulations depend very much on whether the specific system in question falls under the scope of the regulation at all and in which category it is to be categorised.

The first step for companies is therefore to determine what kind of AI system is planned and whether the scope of the regulation applies in this case. It should be borne in mind that relationships with cooperation partners, for example, may also be relevant for this assessment. This is particularly the case if a product consists of different modules that are manufactured by different co-operation partners.[1938] In addition, the entire entrepreneurial field of activity must be analysed, which may also include areas such as development, marketing and the company's internal and external communication (e.g. with chatbots) as well as the product-independent use of AI systems such as *ChatGPT* or *DeepL Translator*. [1939]

The second step is to determine the level at which the AI is categorised in the regulation's risk-based system. Legal and technological advice should be sought at an early stage to ensure appropriate categorisation.[1940] The relevant requirements and obligations must then be identified and implemented.

It is generally advisable to build up your own in-house expertise or seek external support.[1941] For example, the implementation of the necessary compliance management systems based on the requirements of the regulation can then be started at an early stage. Consideration should also be given to the numerous documentation obligations and, in particular for reporting obligations, time should be planned for contact with the authorities and deadlines should be observed.[1942]

It is also important not to forget the various regulations in addition to the AIA, which can also become relevant when using AI: In particular, legal requirements or contractual agreements on liability, attribution and copyright issues as well as the handling of data must always be taken into account. The use of AI can therefore result in a complex overall picture of requirements and obligations.

1938 Frost, Y./Steiniger, M./Vivekens, S., *MPR* 2024, 18.
1939 Frost, Y./Steiniger, M./Vivekens, S., *MPR* 2024, 18.
1940 Frost, Y./Steiniger, M./Vivekens, S., *MPR* 2024, 18.
1941 Chibanguza, K./Steege, H., *NJW* 2024, 1775.
1942 Chibanguza, K./Steege, H., *NJW* 2024, 1775.

B. Function-related regulation

Bibliography

Apel, S., & Huber, C., "Das neue Datenrecht der EU – Eine Übersicht," *JuS* (2024), 514; Drewes, H., Meyer, L., & Moss, P., "Update: Europäische Plattformregulierung – Die ersten Schritte von DMA und DSA in der Praxis," *RDi* (2024), 310; Podszun, R. (ed.), Digital Markets Act, Handkommentar, 1st ed., Nomos 2023; Steinrötter, B. (ed.), Europäische Plattformregulierung, 1st ed., Nomos 2023.

The ongoing digitalisation of markets has led to an enormous increase in data exchange. The collection, processing and transmission of (user) data in the European Union and beyond is largely due to platforms such as social networks and online marketplaces that collect and analyse the collected data.[1943] These data sets ultimately lead to a **concentration of power** on the part of the data holders by giving the respective platform a competitive advantage over competitors on the one hand and providing deep insights into user behaviour on the other.[1944] Overall, this data sovereignty of the platforms reinforces structural imbalances, as it makes it more difficult for new players to enter the market and puts competing companies that do not have the same amount of data resources at a disadvantage.[1945]

The European Commission recognised the resulting systemic risks to competition and consumer protection in the digital single market and launched a legislative package in 2020 consisting of the Digital Services Act[1946] and the Digital Markets Act[1947] .[1948] The legislation aims to curb the market power of large platforms (so-called **gatekeepers**) and create a safe online environment for consumers. Similarly, the **Platform-to-Business Regulation**[1949], which was adopted in 2019, aims to ensure fairness and transparency in the B2B sector.[1950] As the addressees of all legal acts are always platforms in the broader sense, the regulations are collectively referred to as **European platform regulation**[1951].[1952]

The European legislator has opted for a function-based **approach** to platform regulation, which, in contrast to product-based regulation, is not linked to specific characteristics of a product, but to the specific activities and functions of the platforms. One example that can be used to illustrate the function-based

1943 COM(2020) 66 final.
1944 COM(2020) 66 final.
1945 COM(2020) 66 final.
1946 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC, OJ L 277, 27.10.2022, p. 1-102.
1947 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ L 265, 12.10.2022, p. 1-66.
1948 https://www.consilium.europa.eu/de/policies/digital-services-package/ (last accessed on 1 November 2024).
1949 Regulation (EU) No 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11.7.2019, pp. 57-79.
1950 See Art. 1(1) Regulation (EU) 2019/1150.
1951 Steinrötter, B., Europäische Plattformregulierung, 1st ed. 2023, Foreword; however, this is not a clearly definable area of law, Drewes, H./Meyer, L./Moss, P., *RDi* 2024, 310 (310).
1952 The term Union data law is also occasionally used, Apel, S./Huber, C., *JuS* 2024, 514 (514).

regulatory approach is **Art. 5(2)(a)–(d) DMA**, which prohibits companies classified as gatekeepers from combining and using data from different services without the qualified consent of the user. The legislator thus regulates the specific activity of platforms by prohibiting the commercialisation of end user data in advance.[1953] Overall, focussing on the specific functionality of platforms and their business models helps to better identify and combat potential cases of abuse, which ultimately helps to strengthen users' trust in online platforms and marketplaces.

[1953] Podzun, R., DMA, 1st ed 2023, Art. 5(2) para. 10, 11.

IV. Platform-to-Business Regulation (P2BR) - Regulation (EU) 2019/1150

Bibliography

Alexander, C., "Anwendungsbereich, Regelungstechnik und einzelne Transparenzvorgaben der P2B-Verordnung," *WRP* (2020), 945; Busch, C., "Der Digital Services Act: Ein neuer Rechtsrahmen für den Online Handel?" *ZdiW* (2021), 88; Busch, C., Verordnung (EU) 2019/1150 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (P2B-VO), 1st ed., Nomos 2022; Dewenter, R., Haucap, J., & Kehder, C. (eds.), Wettbewerb und Regulierung in Medien, Politik und Märkten – Festschrift für Jörn Kruse zum 65. Geburtstag, Nomos 2013; Eickemeier, D., & Brodersen, C., "Die neue P2B-VO," *K&R* (2020), 397; European Commission, "Questions and Answers – Establishing a Fair, Trusted and Innovation Driven Ecosystem in the Online Platform Economy," accessible at https://www.bundesnetzagentur.de/EN/Areas/Digitalisation/P2B/_func/FAQ_EU.pdf?__blob=publicationFile&v=3; Fritzsche, J., Münker, R., & Stollwerck, C. (eds.), Beck'scher Online-Kommentar UWG, 26th ed., Status: 1 July 2024, C.H. Beck; Höpper, T., & Schulz, A., "Die EU-Verordnung ('PZB-Verordnung') für Fairness und Transparenz von Online-Vermittlungsdiensten 2019/1150," *ZIP* (2019), 2329; Kohser, K., & Jahn, S., "Die P2B-Verordnung – Neue Pflichten für Plattformbetreiber und Suchmaschinenanbieter," *GRUR Prax* (2020), 273; Köhler, H., Bornkamm, J., & Feddersen, C. (eds.), Gesetz gegen den unlauteren Wettbewerb, 14th ed., Band 13a, C.H. Beck 2024; Metzger, A., Vetter, S., & Witte, Z., "Art. 12 der neuen EU-P2B-Verordnung – Die Benennung von Schlichtungsstellen als Mediatoren," *CR* (2020), 739; Müller-Terpitz, R., & Köhler, H., *DSA*, 1st ed. Nomos 2024; Neumann, M., & Rodenhaus, S., "Die P2B-Verordnung aus Unternehmersicht," *ZEuP* (2020), 768; Paal, B., & Pauly, D. A. (eds.), DS-GVO, BDSG, 3rd ed., C.H. Beck 2021; Schneider, R., & Kremer, F., "Ein zweiter, kritischer Blick auf die P2B-Verordnung: Nachhaltige Veränderung des Plattformökosystems?" *WRP* (2020), 1128; Steinrötter, B., *Europäische Plattformregulierung*, 1st ed., Nomos 2023; Tribess, H., "Datenzugangsrechte in der Plattformökonomie – Auswirkungen der P2B-Verordnung im Bereich datenschutzrechtlicher Transparenzpflichten," *ZD* (2020), 440; Tribess, H., "P2B-Verordnung zur Förderung von Fairness und Transparenz von Online-Diensten," *GWR* (2020), 233; Voigt, T., & Reuter, C., "Plattform-to-Business-VO," *MMR* (2019), 783; v. Westphalen, F., "B2B-Plattform-Verordnung," *BB* (2020), 579; v. Westphalen, F., Thüsing, G., & Pamp, J. (eds.), Vertragsrecht und AGB-Klauselwerke, 50th ed., C.H. Beck 2024; Wais, H., "B2B-Klauselkontrolle in der Plattform-Ökonomie," *EuZW* (2019), 221.

1. Introduction

The Platform-to-Business Regulation (hereinafter: P2BR) regulates the relationship between business users and online platforms on which users can offer their goods or services to consumers. The regulation came into force on 31 July 2019 and has been directly applicable in all member states since 12 July 2020. It creates rules on fairness and transparency by imposing obligations on the operators of online platforms. The P2BVO -thus regulates the behaviour of platforms in the digital single market and is part of the European Commission's **digital strategy**.[1954]

[1954] COM(2015) 192 final.

a) Backgrounds

In recent decades, the internet has had a major impact on the economy and trade. Digital distribution enables or facilitates access to the single market and creates new business opportunities.[1955]

Online platforms such as social networks, marketplaces and search engines offer their services to bring together commercial providers of goods or services and their potential customers for the purpose of concluding a contract.[1956] Providers benefit from greater reach and visibility, while consumers are offered a large selection of providers.[1957] The online platforms serve as **gatekeepers** for consumers to access the offers on the market.[1958] In addition, providers can compare their offers with competing products and thus make their offers appear more attractive, while customers can compare offers more easily.[1959]

The online platforms offer commercial users advantageous access to the market and potential customers, but this also harbours the risk of a certain dependency on the online platforms for them.[1960] This can be seen particularly clearly in the example of rankings, which determine which offers are displayed to customers and in what order. Rankings have a huge impact on visibility to customers and therefore also on purchasing decisions, but are created independently by the operators of the online platforms.[1961] The P2BR aims to regulate this dependency and strengthen the rights of commercial users. In particular, this is to be supported by the mandatory introduction of complaint management systems, which have been lacking on a regular basis to date.[1962]

The focus is particularly on small and medium-sized enterprises (SMEs), as they lag behind large companies or groups both in terms of their structure and their resources (personnel, economic weight).[1963] Consumer protection is also extended by the provisions of the P2BR, but is only an indirect objective, as this is already primarily realised by other European regulations.[1964]

1955 Rec. 1 Regulation (EU) 2019/1150.
1956 Rec. 11 Regulation (EU) 2019/1150.
1957 Rec. 1 Regulation (EU) 2019/1150.
1958 Rec. 12 Regulation (EU) 2019/1150.
1959 Voigt, T./Reuter, C., *MMR* 2019, 783 (783).
1960 Voigt, T./Reuter, C., *MMR* 2019, 783 (783).
1961 Rec. 24, 26 Regulation (EU) 2019/1150.
1962 Rec. 5 Regulation (EU) 2019/1150.
1963 COM(2003) 1422.
1964 Rec. 3 Regulation (EU) 2019/1150.

b) Goals

The regulation aims to restrict unfair practices by online platforms and create remedial mechanisms to strengthen the internal market.[1965] In its proposal for a regulation on transparency and fairness for business users of online intermediation services[1966], the Commission proposed rules on transparency obligations and procedural rules.[1967] Parliament, on the other hand, was in favour of formal transparency obligations as well as substantive fairness requirements, but was outvoted in the trilogue procedure.[1968]

The core areas of the regulation are the creation of sufficient transparency regarding the creation of rankings, contract cancellations[1969] and the restriction of services on the market.[1970] On the other hand, this transparency is intended to increase the trust of commercial users in the platforms. This trust, in combination with protection against unfair practices[1971], should benefit the internal market.

The Regulation defines different obligations to be complied with for different types of online platforms. It differentiates between online intermediary platforms (Art. 2 No. 2 P2BR) and online search engines (Art. 2 No. 5 P2BR), whereby most of the regulations are laid down for online platforms. Particular importance is attached to the design of general terms and conditions (Art. 3 P2BR). According to Art. 5 P2BR, special transparency provisions apply to all online platforms for the rankings they create. A special feature is the introduction of a representative action in Art. 14 P2BR, which enables commercial users to file an action for injunctive relief via an association or organisation in the event of infringements against the platform.

c) Differentiation from other legal acts of platform regulation

The P2BR was supplemented by the DSA and the DMA in 2022 in order to adequately protect free competition.[1972] The DMA formulates in Art. 5 et seq. DMA formulates strict prohibitions and bans, which are also directed exclusively at gatekeepers. The DSA distinguishes between different types and sizes of intermediary services. It is also based on the provisions of the P2BR for complaints management and out-of-court dispute resolution (Art. 11, 12 P2BR). The P2BR is therefore regarded as a model for the DMA and DSA that were issued later. The P2BR supplements national antitrust regulations and does not supersede them.[1973]

1965 Rec. 6 Regulation (EU) 2019/1150.
1966 COM(2018) 238 final.
1967 Busch, C., P2B-VO, 1st ed. 2022, Introduction para. 4.
1968 Busch, C., P2B-VO, 1st ed. 2022, Introduction para. 8.
1969 Rec. 23 Regulation (EU) 2019/1150.
1970 Rec. 22 Regulation (EU) 2019/1150.
1971 Rec. 30, 31 Regulation (EU) 2019/1150.
1972 Busch, C., P2B-VO, 1st ed. 2022, Introduction para. 15.
1973 Alexander, C., *WRP* 2020, 945 (949).

2. Scope, Art. 1(1), (2) P2BR

a) Personal scope

Pursuant to Art. 1(1) P2BR, the Regulation applies to legal relationships in connection with the conclusion of contracts via online platforms. There are basically three legal relationships: The platform usage relationship on the customer side, the platform usage relationship on the provider side and the customer-provider relationship.[1974]

aa) The customer relationship

The customer relationship exists between the **platform** and the customer using the platform. There must therefore be at least a de facto user relationship.[1975] Recital 9 P2BR states that the Regulation only applies if the customer's platform usage relationship is with a **consumer**.[1976] A consumer within the meaning of the Regulation is a natural person who is not acting on the market for the purposes of a trade, business, craft or profession.[1977]

bb) The supplier-side relationship

The provider-side platform usage relationship exists through a contractual relationship between the platform and the **provider who offers its goods or services to a consumer via the platform**.[1978] Although the P2BR indirectly strengthens consumer protection, only these providers are directly protected.[1979] The provider must be either **a business user** or a **user with a company website**.[1980]

According to Art. 2 No. 1 P2BR, business users are legal entities or private individuals who offer goods or services to consumers in connection with their commercial, business, craft or professional activity via online intermediary service providers. The term "professional activity" should be read as an independent professional activity.[1981] In particular, commercial enterprises are to be covered by the regulation.[1982] Even if the wording only requires a connection between the offering and the activity, this must be read as part of the activity.[1983]

Users with a business website are natural or legal persons who offer goods or services to consumers via an online interface for purposes relating to their trade, business, craft or profession, in accordance with Art. 2(7) P2BR. An online interface is defined very broadly as software, which includes websites, parts of websites and applications, including mobile applications, Art. 2 No. 7 P2BR.

1974 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 24.
1975 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 24.
1976 See also Rec. 2, 3, 4 of Regulation (EU) 2019/1150.
1977 Rec. 12 Regulation (EU) 2019/1150.
1978 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 24.
1979 Rec. 3 Regulation (EU) 2019/1150; see also CJEU. 30. Sept. 2024, case C-664/22, C-666/22 = *NJW* 2024, 2165.
1980 Art. 1(1) P2B-VO.
1981 Busch, C./Schulte-Nölke, H., P2B-VO, 1st ed. 2022, Art. 2 para. 6.
1982 Busch, C./Schulte-Nölke, H., P2B-VO, 1st ed. 2022, Art. 2 para. 6.
1983 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 9.

cc) The customer-provider relationship

The customer-provider relationship already arises through the initiation of a transaction between the customer and the provider of the online platform.[1984] B2B and C2C contracts are excluded due to the above-mentioned consumer status of the customer and the provider's status as a commercial user. This is only convincing on the assumption that companies offering goods or services to other companies are large enough to be on an equal footing with the platform providers, i.e. that there is no power imbalance. However, there are no strong reasons for such an assumption, especially not when SMEs contract with each other.[1985] If an SME offers goods or services to another SME as a commercial user, there is no protection under the P2BR for the former. Whether such a protection gap will last in the long term remains to be seen.

b) Material scope, Art. 2 P2BR

The P2BR applies to providers of **online intermediary services** and **online search engines** (online platforms) as addressees of the standard.[1986] The majority of the regulation governs contractual relationships for online intermediary services, while there are only a few provisions for online search engines.

The size of the platform plays no role in the P2BR as it does in the DMA. In contrast to the DMA, only the structural power of the platform operators to conclude contracts is relevant in the P2BR for the assessment of power positions, not the economic size.[1987] This means that, in principle, SMEs also fall under the scope of the regulation as platform operators; however, they do not have to set up an internal complaints management system or specify mediators in their general terms and conditions, but may do so voluntarily.[1988]

aa) Online intermediary services, Art. 2 No. 2 P2BR

(1) Definition

The P2BR provides its own definition of intermediary services in Art. 2 No. 2, which the European legislator did not take up verbatim in the DSA that was subsequently issued. For an online intermediary service to exist, the requirements listed below must apply cumulatively in accordance with Art. 2 No. 2 P2BR.

1984 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 24.
1985 Voigt, T./Reuter, C., *MMR* 2019, 783 (784).
1986 Art. 1(1) P2BR.
1987 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 17.
1988 Rec. 38, 41 Regulation (EU) 2019/1150.

(a) Service of an information society, Art. 2 No. 1(a) P2BR

Firstly, according to Art. 2 No. 2(a) P2BR, an information society service within the meaning of Art. 1(1)(b) Directive 2015/1535/EN must be present. This is the case if the service is provided individually on demand, at a distance and electronically.[1989] The term "service" is congruent with the term used in the fundamental freedoms under Art. 56, 57 TFEU.[1990]

As a rule, this service must be provided in return for payment. Payment is to be understood broadly and does not necessarily require remuneration of the platform operator by the commercial user.[1991] According to ECJ case law, a service is provided for remuneration if it is commercially oriented,[1992] i.e. it is not necessary for the user to pay a direct fee.[1993] It is equivalent to monetary consideration if the user pays with their personal data.[1994] On the one hand, this results from the inherent economic value of personal data.[1995] Secondly, from a systematic view of other Union legal acts: For example, Art. 3(1)(2) Digital Goods Directive 2019/770 also explicitly covers the provision of personal data as consideration and equates this to a payment.

A service is individualised on demand if it is provided by the transmission of data on individual request, Art. 1(1)(b) No. iii Directive 2015/1535/EN. The recipient of the service therefore makes a request, which is then transmitted by the service provider to the data compiled for the recipient[1996] (i.e. not point-to-multipoint transmission).[1997] According to Art. 1(1)(b)No. i Directive 2015/1535/EN, a service is provided at a distance if it is provided without the simultaneous physical presence of the contracting parties.[1998] The service is provided electronically in accordance with Art. 1(1)(b)(i) Directive 2015/1535/EN if it is sent and received entirely by means of equipment for the electronic processing and storage of data, i.e. the service is provided via an electronic communications network.[1999] The scope therefore excludes services that are only provided with the aid of electronic equipment but not entirely by means of such equipment.[2000]

1989 Art. 1(1)(b) Directive 2015/1535/EN.

1990 CJEU, 3 Dec. 2020, case C-62/19, para. 43 - Star Taxi App = *MMR* 2021, 309.

1991 Rec. 18 Directive 2000/31/EC.

1992 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 7; Dreier, T./Schulze, G./Raue, B., UrhDaG, 7th ed. 2022, § 2 para. 6.

1993 CJEU, 11 Sept. 2014, case C-291/13, para. 28 et seq. – Papasavvas = *MMR* 2016, 63; CJEU, 15. Sep. 2016, case C-484/14para. 41 - McFadden/Sony = *GRUR* 2016, 1146; CJEU, 4 May 2017, case C-339/15, para. 36 – Vanderborght = *GRUR* 2017, 627.

1994 Steinrötter, B./Schauer, L., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 7.

1995 Dreier, T./Schulze, G./Raue, B., UrhDaG, 7th ed. 2022, § 2 para. 11.

1996 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 9.

1997 Paal, B./Pauly, D. A./Ernst, S., DS-GVO BDSG, 3rd ed. 2021, Art. 4 para. 147.

1998 With regard to the P2B-VO, this means a distance contract between the platform and the commercial user.

1999 Art. 1(1)(b)(ii) Directive (EU) 2015/1535; Steinrötter, B./Schauer, L., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 8.

2000 Steinrötter, B./Schauer, L., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 8.

(b) Mediation of the initiation of transactions between business users and consumers

The service of the information society would then have to be aimed at an intermediary activity, i.e. mediating a transaction between customers and commercial users.[2001] This does not depend on the (effective) conclusion of a contract, but merely on the initiation and preparation of such a transaction.[2002] Transactions are all processes that prepare or at least hold out the prospect of a contract being concluded.[2003] The fact that the platform provides a framework in which goods and services can be offered already constitutes mediation. The platform operators must be interested in facilitating a transaction, and this is not only possible by chance (as is the case with telecommunications services).[2004]

(c) Provision of brokerage by contractual basis, Art. 2 No. 2(c) P2BR

According to Art. 2 No. 2(c) P2BR, an online intermediary service only exists if the service is based on a contract with the business user.

(aa) Effectiveness of the contract

The regulation itself does not contain any clear rules on this. Recital 10 P2BR only requires an expression of intent, i.e. not the effective conclusion of a contract.[2005] Furthermore, Art. 2 No. 2(c) P2BR merely states that the service is provided on the basis of a contractual relationship, but not on the basis of a contract. Nevertheless, the objective of the regulation must be taken into account: The provider's contractual obligations (especially in general terms and conditions) are to be set out transparently. However, the commercial user can only be adequately protected if he can also enforce this in court.[2006] An effective conclusion of contract is therefore required for the regulation to apply. In principle, it is irrelevant in which legal system the contract was concluded, i.e. also according to the law of third countries (according to the ROM I Regulation).[2007] However, the choice of law of the contract plays a role if the validity of the contract has to be reviewed,[2008] for example if a court has to review the validity of a contract from another legal system for the applicability of the Regulation.

(bb) Declaration on a durable medium, Art. 2 No. 13 P2BR

According to recital 10 P2BR, the intention to be bound must be stored on a durable medium. According to Art. 2 No. 13 P2BR, this is the case if the commercial user's information can be accessed, viewed and retrieved for a reasonable period of time. However, it is questionable whether the requirement of a durable medium is constitutive for an intermediary activity within the meaning of the Regulation.

2001 Art. 2 No. 2(b) P2BR.
2002 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 25.
2003 Busch, C./Schulte-Nölke, H., P2B-VO, 1st ed. 2022, Art. 2 para. 29.
2004 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 27.
2005 See also European Commission, Q&A EN Communication 2020, p. 12.
2006 Busch, C./Schulte-Nölke, H., P2B-VO, 1st ed. 2022, Art. 2 para. 43.
2007 Busch, C./Schulte-Nölke, H., P2B-VO, 1st ed. 2022, Art. 2 para. 39.
2008 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 29.

On the one hand, this could be affirmed, because effective protection of the commercial user is only guaranteed if the user can prove the conclusion of a contract, which is easily possible through storage. [2009]

On the other hand, storage on a durable medium cannot play a role in the applicability because the provider would then unilaterally determine the applicability through its contract conclusion requirements and the user would not be protected.[2010] In addition, the requirement of the recital is merely intended to distinguish it from other formal requirements (from the respective legal system of the contract conclusion). [2011]

The storage requirement could also be understood as a unilateral option for the user, who can release themselves from their obligations if this is not the case.[2012] Sanctions in the event of a breach could then be imposed by other instruments (for example in competition law).[2013] The dispute remains open for the time being.

(2) Examples

Most online intermediary services fall under the definition, meaning that the target group is very broad. Nevertheless, the regulation is mainly aimed at the large platforms (*gatekeepers*), as the greater the difference between the platform and the commercial user, the more dangerous an abuse of power can be.[2014] The so-called **GAFA platforms**[2015] (‘Google‘, ‘Amazon‘, ‘Meta‘ formerly ‘Facebook‘,‘Apple‘) are particularly in focus.[2016] Well-known examples of online brokerage platforms are comparison portals (‘Check24‘) or product search engines (‘idealo‘) and sales portals (‘Amazon Marketplace‘, ‘Google Shopping‘, ‘Meta Marketplace‘, ‘ebay‘).[2017] However, platforms that are aimed at terminating, changing or asserting secondary claims (‘Kündigen.com‘, ‘Aboalarm‘) are not included.[2018]

bb) Online search engines, Art. 2 No. 5 P2BR

In addition to the online brokerage platforms, operators of online search engines are also addressees of the P2BR, although they are obliged to a limited extent.

According to Art. 2 No. 5 P2BR, online search engines are digital services that enable users to enter a keyword, voice input or phrase in order to perform a search on any topic on any website and have the results displayed. This definition is basically congruent with that of the DSA, whereby the legislator has

---

2009 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 33.
2010 Busch, C./Schulte-Nölke, H., P2B-VO, 1st ed. 2022, Art. 2 para. 47; a.A. Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 33.
2011 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 33.
2012 Busch, C./Schulte-Nölke, H., P2B-VO, 1st ed. 2022, Art. 2 para. 47.
2013 Busch, C./Schulte-Nölke, H., P2B-VO, 1st ed. 2022, Art. 2 para. 47.
2014 Neumann, M./Rodenhaus, S., *ZEuP* 2020, 768 (776).
2015 https://inztitut.de/blog/glossar/gafa/ (last accessed on 1 November 2024).
2016 Neumann, M./Rodenhaus, S., *ZEuP* 2020, 768 (776).
2017 https://ec.europa.eu/commission/presscorner/api/files/document/print/de/ip_23_4328/IP_23_4328_DE.pdf (last accessed on 1 November 2024).
2018 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 25.

dispensed with the term intermediary service here, so that the problem of categorising online search engines does not arise here, in contrast to the explanations on the DSA.[2019]

Online search engines are not a service in the sense of an information society. It remains unclear what exactly is meant by digital. The service must be based on "information expressed in digits".[2020] Furthermore, no remuneration is required here. It is also important that the search engine processes the search queries on all websites and is not limited either thematically or to specific sources.[2021]

An important difference in contrast to online intermediary services is that there are only **two legal relationships** when using online search engines and not three as shown above.[2022] In the case of online search engines, only the de facto user relationship between the search engine and the consumer is relevant, as well as an at least pre-contractual relationship between the consumer and the business website.[2023] **There is no** need for **a contractual relationship** between the **search engine** and the **business website**.[2024]

cc) Territorial scope, Art. 1(1) P2BR

Online platforms can be used worldwide via the internet, which is why it is necessary to take a close look at their geographical applicability. Art. 1(1) P2BR stipulates that the Regulation applies if the service is provided or offered to business users who are established or resident in the EU (**country of establishment principle**) and who offer their services or goods to consumers in the EU (**market place principle**). According to Art. 1(2) P2BR, the place of establishment of the online platform operator is not relevant.

The business user must clearly target its services to consumers from at least one Member State.[2025] This does not depend on the commercial user's intention to do so, but on the circumstances of the individual case.[2026] Possible indications may be the use of a Member State domain (or .eu) or telephone number as well as the mention of international customers such as through reviews or similar.[2027]

Consumers, on the other hand, only need to be located in the EU; nationality or residence in a Member State is not required.[2028] As a result, business users who offer their services to consumers outside the EU are not bound by the regulation. In principle, the European legislator is only responsible for European consumer protection, which determines this geographical restriction. However, consumer protection is

---

2019 See DSA definition online search engine.
2020 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 35.
2021 Haucap, J./Kehder, C., *FS Kruse* 2013, 115 (119).
2022 For online intermediary service providers, see Art. 2 No. 2(c) Regulation (EU) 2019/1150.
2023 Steinrötter, B./Arncken, D., Europäische Plattformregulierung, 1st ed. 2023, § 16 para. 34.
2024 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 1 para. 21.
2025 The consumer must be located in the EU for at least part of the transaction, Rec. 9 Regulation (EU) 2019/1150.
2026 CJEU, 7 Dec. 2010, C-585/08. and C-144/09, EU:C:2012:740, para. 83 - Pammer and Hotel Alpenhof.
2027 CJEU, 7 Dec. 2010, C-585/08. and C-144/09, EU:C:2012:740, para. 83 - Pammer and Hotel Alpenhof.
2028 Rec. 9 Regulation (EU) 2019/1150.

only an indirect objective of the regulation; the focus is on protecting commercial users from the superiority of the platform provider.[2029] This protection is not possible if a business user only targets consumers from third countries.[2030] Thus, the location of the consumer determines the need for protection of the commercial user.[2031] This means that market power can be abused by platform operators without possible consequences under the P2BR.[2032] This may be questionable if the operator of the online platform is also based in the EU, as there is then in any case a connection to the internal market in accordance with Art. 114(1) TFEU and the legislator could therefore adopt a standardised regulation for platforms used in the EU.[2033]

3. Requirements for online brokerage services and online search engines

a) Online brokerage services

The P2BR lays down most of the rules for providers of online intermediary services. These will be considered individually below before the obligations of online search engines are discussed.

aa) GTC, Art. 3 P2BR

Art. 3 P2BR is the main focus of the Regulation and regulates the requirements to be met by the GTCs provided by online platforms. Providers of online intermediary services regularly use general terms and conditions. The P2BR specifies how exactly the T&Cs must be presented to the business user and what content they must contain.

With the Directive/93/13/EEC (Directive on standard terms and conditions)[2034], the European legislator introduced the standardisation of legal provisions on standard terms and conditions as early as 1993. The aim of this was to standardise the internal market and thus strengthen consumer protection.[2035] However, the provisions of the Directive do not apply directly to the GTC of online platforms, as these only apply to the GTC of consumer contracts, whereas the P2BR regulates the supplier-side relationship between two companies.[2036] The Member States have the option of tightening up the provisions of the Directive through the transposition laws of the Clauses Directive, so that B2B contracts can also fall under the control of clauses in national law.[2037] However, the P2BR creates standardised transparency regulations for the drafting of **general terms and conditions between two companies** in the EU for the first time, but refers specifically to the obligations for online platforms.

2029 Rec. 3 Regulation (EU) 2019/1150.
2030 Wais, H., *EuzW 2019*, 221 (222).
2031 Voigt, T./Reuter, C., *MMR* 2019, 783 (784).
2032 Wais, H., *EuzW 2019*, 221 (222).
2033 Wais, H., *EuzW 2019*, 221 (222).
2034 Directive (EU) 1993/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ NoOfficial Journal of the European Communities, OJ L 95, 21.4.1993.
2035 Rec. 2 Directive 93/13/EEC.
2036 See under 2. a).
2037 For example, in German law this is standardised in § 310(1) of the German Civil Code, in Italian law Art. 1341, 1342 Codice Civile apply to all contracts (e contrario Art. 33 et seq. Codice del Consumo).

In Art. 2 No. 10 P2BR, GTCs are formulated differently from the Clauses Directive, but are similar to this definition.[2038] The P2BR does not require that the GTCs are pre-formulated, nor that they are used in a large number of contracts. Art. 2 No. 10 P2BR stipulates that the GTC are unilaterally determined, but not that they are unilaterally included.[2039] Nevertheless, only the T&Cs of the online intermediary service are covered by the P2BR, while the national provisions apply to the (albeit rarely used) T&Cs of commercial users.[2040]

(1) Obligations to include general terms and conditions, Art. 3 (1) P2BR

Firstly, certain requirements are placed on the manner in which the GTCs are included. According to Art. 3(1)(a) P2BR, the GTC must be formulated in a clear and comprehensible manner.[2041] In addition, the T&Cs must be easily available to the business user (Art. 3(1)(b) P2BR). The required availability must be guaranteed for both existing and potential future contractual partners.[2042] This is already fulfilled by a link on your own website.[2043]

Furthermore, the content requirements to be introduced by the providers are regulated. Art. 3(2)(c) P2BR requires providers to state in their T&Cs the reasons for which the provision of the platform may be suspended, terminated or restricted.[2044] This stipulates that the effectiveness of such measures only becomes effective through the justification in accordance with Art. 3(2)(c) P2BR.[2045] Furthermore, commercial users should receive information about additional distribution channels or partner programmes of the intermediary services in accordance with Art. 3(1)(d) P2BR in order to know through which the platform may still distribute the users' offers.[2046] Finally, the effects on the ownership of intellectual property of commercial users must be noted, Art. 3(1)(e) P2BR. The intellectual property in their own products is of considerable economic importance for commercial users, meaning that the possible effects of the GTC on this must be presented transparently.[2047] The Regulation cites the use of logos, trademarks and business names as examples.[2048] In addition, the inclusion of information on the points listed in Art. 5 et seq. P2BR.

(2) Obligations in the event of changes to the GTC, Art. 3(2) P2BR

Art. 3(2) P2BR sets out requirements for amendments to the GTC. The platform operator may propose changes to its GTC to the business user. Amendments must be submitted on a durable medium.[2049]

2038 Art. 3(2) Directive 93/13/EEC.
2039 Eickemeier, D./Brodersen, C., *K&R* 2020, 397 (398).
2040 v. Westphalen, F., *BB* 2020, 579 (579).
2041 See Art. 5 Directive 93/13/EEC.
2042 Rec. 18 Regulation (EU) 2019/1150.
2043 Schneider, R./Kremer, F., *WPR* 2020, 1128 (1132); Voigt, T./Reuter, C., *MMR* 2019, 783 (784).
2044 More details below under Art. 4 Regulation (EU) 2019/1150.
2045 Busch, C./v. Westphalen, F., P2B-VO, 1st ed. 2022, Art. 4 para. 1.
2046 Rec. 16 Regulation (EU) 2019/1150.
2047 Rec. 17 Regulation (EU) 2019/1150.
2048 Rec. 17 Regulation (EU) 2019/1150.
2049 See 2. b) aa) (1) (c) (bb).

However, this does not include purely editorial changes if these do not change the content and meaning of the clause.[2050]

The commercial user then has the option of cancelling the contract within a certain period of time. This period is 15 days from notification of the change, but may be longer in individual cases in accordance with Art. 3(4) P2BR.[2051] However, any shorter national deadlines must be observed.[2052]

However, commercial users have the right to waive the time limit entirely in accordance with Art. 3(2) P2BR. This is possible either through a written declaration or a clearly confirming act. The re-listing of goods or services is to be regarded as a confirmatory act.[2053] If an extended deadline applies due to special circumstances, the posting is not considered an implied waiver of the deadline.[2054]

(3) Nullity of general terms and conditions, Art. 3(3) P2BR

If the GTC violate one of the provisions mentioned in (1) and (2), they shall be null and void pursuant to (3). This nullity shall be effective ex tunc erga omnes against all contracting parties.[2055] This also rules out recourse to dispositive substitute law.[2056] Nevertheless, only the provision that does not fulfil the requirements is null and void. If other provisions are separable from the void provision, they continue to exist.[2057]

A special feature is Art. 8 P2BR, which as a substantive legal standard sets out requirements for the use of clauses. It stipulates that no retroactive changes are to be made to the T&Cs, that the T&Cs must include termination options for commercial users and that data protection requirements must be set out. In contrast to Art. 3 P2BR, it does not contain its own nullity provision, meaning that infringements are governed by the applicable national law.[2058]

(4) Competitions

According to Art. 1(4) P2BR, the general civil law of the Member States remains unaffected. In principle, the national regulations on general terms and conditions and their control continue to apply and must be supplemented by the P2BR.[2059] It must always be clarified whether the P2BR -provides a conclusive regulation for a specific behaviour. [2060] If this is not the case, the relevant substantive law must

---

2050 Rec. 18 Regulation (EU) 2019/1150.
2051 For example, if the GTC require extensive restructuring by the user, Art. 3(2) Regulation (EU) 2019/1150, see also Art. 3(4) Regulation (EU) 2019/1150.
2052 Rec. 18 Regulation (EU) 2019/1150.
2053 Rec. 19 Regulation (EU) 2019/1150.
2054 Rec. 19 Regulation (EU) 2019/1150; Wais, R., 'P2B-VO Art. 3', in: BeckOK UWG (26th ed. 2024) para. 42.
2055 Rec. 20 Regulation (EU) 2019/1150.
2056 v. Westphalen, F., *BB* 2020, 579 (585).
2057 Rec. 20 Regulation (EU) 2019/1150.
2058 Höpper, T./Schulz, A., *ZIP* 2019, 2329 (2235), Schneider, R./Kremer, F., *WPR* 2020, 1128, (1130-1131).
2059 Kohser, K./Jahn, S., *GRUR Prax* 2020, 273 (275).
2060 v. Westphalen, F./Thürsig, G./Pamp, J./Hoeren, T., Vertragsrecht und AGB-Klauselwerke, 50th ed. 2024, para. 125.

be applied.[2061] Nevertheless, the interpretation of the P2B standards as European regulatory law must always be interpreted autonomously.[2062] This also applies if other legal issues relating to the same facts are to be clarified in accordance with the principles of private international law under a specific legal system.[2063]

bb) Restriction, suspension and termination, Art. 4 P2BR

Art. 4 P2BR stipulates that providers must provide their users with written reasons why they are restricting, suspending or terminating the provision of their own services for the user's products. Such a restriction, suspension or termination is only justified by legitimate reasons.[2064] These reasons are already mentioned in Art. 3(1)(c) P2BR, so that Art. 4 P2BR stipulates above all that the reasons must be recorded on a durable medium, Art. 3(1) P2BR. Art. 4(5) P2BR specifies the obligation to state reasons to the effect that the platform operator must include all specific facts and circumstances, both factual and legal.[2065] In addition, communications from third parties that have influenced the provider's decision must be included. In particular, this may include (negative) criticism from consumers, but also communications from consumer organisations or authorities, as long as there is a direct link to the commercial user or their offer.[2066] In accordance with Art. 4(2) P2BR, the reasons for termination must be provided on the data carrier at least 30 days before the termination takes effect.

According to Art. 4(5) P2BR, the obligation to provide reasons is excluded if the platform operator is not allowed to disclose the reasons due to a legal or official order or if the user has repeatedly (i.e. at least twice) violated the GTC. In the absence of information to the contrary, it can be assumed that there is no repetition if the first offence is time-barred under applicable national law.[2067] In order to be able to invoke the exclusion of the obligation to state reasons, the T&C that violated Art. 4 P2BR must be valid under national law.[2068]

cc) Rankings, Art. 5 P2BR

(5) Regulatory objective

Another key provision of the Regulation is Art. 5 P2BR, which sets out transparency requirements for the process and the creation of the **rankings** produced by online intermediary services.

According to Art. 2 No. 8 P2BR, rankings are the relative prioritisation of goods and services offered on online platforms. The ranking criteria (according to an algorithm or other evaluation mechanism) are determined by the operators of the online intermediary platform.[2069]

2061 For example: Rec. 36 Regulation (EU) 2019/1150.
2062 Alexander, C., *WRP* 2020, 945 (950).
2063 Busch, C./Schulte-Nölke, H., P2B-VO, 1st ed. 2022, Art. 1 para. 45 et seq.
2064 Rec. 22 Regulation (EU) 2019/1150.
2065 Busch, C./v. Westphalen, F., P2B-VO, 1st ed. 2022, Art. 4 para. 29.
2066 Busch, C./v. Westphalen, F., P2B-VO, 1st ed. 2022, Art. 4 para. 29.
2067 Busch, C./v. Westphalen, F., P2B-VO, 1st ed. 2022, Art. 4 para. 34.
2068 Busch, C./v. Westphalen, F., P2B-VO, 1st ed. 2022, Art. 4 para. 37.
2069 Voigt, T./Reuter, C., *MMR* 2019, 783 (783).

The rankings of online platforms have a significant influence on consumer choice, to which the commercial success of business users is directly linked.[2070] For this reason, the requirements of Art. 5 P2BR are intended to create predictability for business users and possibly provide an opportunity to optimise the presentation or goods themselves.[2071] Nevertheless, there is no obligation for the operators of online platforms to disclose the detailed functioning of the mechanisms and algorithms used in order to prevent malicious manipulation.[2072] Furthermore, the standard should not be a rigid obligation to specify certain parameters, but should always be adapted to the type of platform and the individual case.[2073]

(2) Specifications

According to Art. 5(1) P2BR, the main parameters and the reasons for their relative weighting must be listed in the GTC (**product-related factors**). This refers to those parameters that determine the ranking. An explanation of the dynamic nature of the ranking should be provided so that predictability is created with regard to certain influences. Examples of main parameters are given both by the Regulation itself and in Annex I of the European Commission's Ranking Transparency Guidelines, Art. 5(7) P2BR.[2074] According to Art. 5(3) P2BR, it must be explained whether and how commercial users can actively influence the ranking by paying a fee and what effect this has on the ranking.[2075]

In addition, according to Art. 5(5) P2BR, **consumer-related** features must also be presented, such as the so-called matching of product features and the interests of consumers, but also the linking of product features with factors such as location, search history, order history, etc.[2076]

The fact that the information on rankings must be listed in the GTC means that the general updating obligation under Art. 3(2) P2BR also applies to these. It is important to note that temporary changes to the main parameters (Black Friday, delivery difficulties, changes to the technical basis) must also be noted.[2077]

(3) Delimitation to Art. 26, 27 DSA

The DSA sets out transparency requirements for platform operators in Art. 26 and 27 DSA.[2078] The requirements of the two regulations are very similar - for example, the information in the general terms and conditions must be formulated clearly and comprehensibly. In addition, both Art. 27(2)(b) DSA and Art. 5(1) P2BR require the justification of the relative weighting of these parameters.

2070 Rec. 24 Regulation (EU) 2019/1150.
2071 COM(2020) 424/1 Introduction 1.1 No. 5; different in the Transparency Directive 2019/22161, where the transparency requirements are intended to protect the consumer.
2072 Rec. 27 Regulation (EU) 2019/1150.
2073 COM(2020) 424/1 Introduction 1.1 No. 8.
2074 COM(2020) 424/1.
2075 Rec. 25 Regulation (EU) 2019/1150.
2076 Busch, C, P2B-VO, 1st ed. 2022, Art. 5 para. 67.
2077 Busch, C, P2B-VO, 1st ed. 2022, Art. 5 para. 39 et seq.
2078 See also II. 3. d) cc) (6 et seq.).

In principle, the provisions of the P2BR apply as *lex specialis* in accordance with Art. 2(4)(e) DSA if overlaps arise.[2079] Nevertheless, it is important that the different objectives of the regulations are recognised: While the P2BR is concerned with the fair participation of commercial users, Art. 27 DSA focuses on the perspective of the recipient user as to why which offers are displayed and how.[2080]

dd) Differentiated treatment, Art. 7 P2BR

(2) Regulatory objective

According to Art. 7(1) P2BR, platform operators must also include explanations on the differentiated treatment of their own and third-party offers in the GTC. This should refer to the so-called self-preferential treatment of hybrid companies[2081], which are both intermediary service providers and competitors for commercial users.[2082] In these cases, there is an increased risk of abuse of market power because the hybrid companies have the economic incentive and the opportunity to favour their own products.[2083] In addition, competition is weakened by the prevention of so-called climbing in the rankings because there are no longer any incentives to improve one's own products.[2084] The same applies to products offered via the intermediary service by commercial users who are under the control of the intermediary service.[2085] This position of control presupposes a certain economic influence, which is particularly present in group structures.[2086]

(2) Specifications

Treatment within the meaning of Art. 7 P2BR are all measures that could potentially have an impact on the success of access.[2087] These are differentiated if the treatment of two offers differs directly or indirectly.[2088] There is an obligation to disclose if the standards of treatment lead to a significantly different treatment of the third-party provider.[2089] Art. 3 P2BR provides some examples of what information is to be disclosed. Accordingly, preferential treatment for access to personal and other data (a), for ranking (b) with regard to the fees already mentioned in Art. 5(c) P2BR and for access to services, functions and technical interfaces (d) must be specified. While these requirements must already be included in the GTCs in accordance with Art. 5 and 9 P2BR, the requirements under Art. 7 P2BR always refer to the context in which they are related to a possible different treatment compared to third-party providers.

2079 COM(2020) 825 final.
2080 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA,1st ed. 2024, Art. 27 para. 16.
2081 Approx. 1/3 of marketplace providers, COM(2017) 229 final para. 104.
2082 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 7 para. 2.
2083 Rec. 30 Regulation (EU) 2019/1150.
2084 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 7 para. 3.
2085 Rec. 30 Regulation (EU) 2019/1150.
2086 Steinrötter, B./Louven, S., Europäische Plattformregulierung, 1st ed. 2023, § 17 para. 106.
2087 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 7 para. 58.
2088 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 7 para. 66.
2089 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 7 para. 67.

ee) Special contractual provisions, Art. 8 P2BR

Art. 8 P2BR sets out contractual provisions that the provider must observe when concluding the contract. According to Art. 8(a) P2BR, the platform provider may not change the GTC retroactively. Exceptions exist if the legislator or an authority so determines.

Providers must also stipulate in the T&Cs how users can terminate the contractual relationship, Art. 8(b) P2BR. The provision thus represents the counterpart to Art. 4 P2BR, whereby a breach of Art. 8 P2BR does not lead to the invalidity of the GTC.[2090] However, there is no obligation to state grounds for termination. Only those reasons must be stated which the platform provider grants to the user.[2091] Art. 8(b) P2BR also does not apply to purely legal termination options; these are subject to national law in parallel to Art. 1(2) Directive 93/13/EEC.[2092] While recital 32 states that the conditions for termination should be proportionate, this material appropriateness is not addressed in Art. 8 P2BR, so that there is only a pure transparency obligation.

According to Art. 8(c) P2BR, the platform provider must also explain what access it will continue to have to the data provided or generated by the user after termination of the contract. In principle, this requirement is in line with Art. 9(1) P2BR, so that reference is made to its explanations. However, Art. 9(1) P2BR refers to the period during the contractual relationship, whereas Art. 8(c) P2BR refers to the period after the contractual relationship.[2093]

ff) Data access, Art. 9 P2BR

(3) Regulatory objective

Online intermediation services are data-based business models in which the access and processing of data is a central element.[2094] Art. 9 P2BR therefore creates transparency requirements regarding access to and handling of data of commercial users. The commercial users should understand from the information whether they can use the data to add value.[2095] However, there is no right of access to this data.[2096] Art. 9(1) P2BR obliges platform providers to specify in the GTC the access and handling of data for business users that are provided or generated by them or consumers when using the platform. Data is provided when it is actively (consciously or unconsciously) introduced and enters the platform provider's access area.[2097] Generating is understood to mean the automatic generation of information through the use of the intermediary service.[2098]

2090 Wais, R., 'P2B-VO Art. 8', in: BeckOK UWG (26th ed. 2024) para. 7.
2091 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 8 para. 12.
2092 Wais, R., 'P2B-VO Art. 8', in: BeckOK UWG (26th ed. 2024) para. 12.
2093 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 8 para. 15.
2094 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 9 para. 1.
2095 Rec. 33 Regulation (EU) 2019/1150.
2096 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 9 para. 128.
2097 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 9 para. 66.
2098 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 9 para. 70.

Data that the platform provider provides itself is therefore excluded from the transparency obligation.[2099] This includes both personal[2100] and other data. Both technical access, i.e. what measures can be used to access the data, and contractual access, i.e. what legal requirements are placed on this, should be included in the GTC.[2101] This primarily concerns the scope, type and conditions under which the commercial user is granted access to the data.[2102] Article 9 of the P2BR does not stipulate that the platform provider must make data available, but the transparency requirements can increase the exchange of data and strengthen the European data space.[2103]

(2) Requirements, Art. 9(2) P2BR

Art. 9(2) P2BR sets out some requirements as to the content of the explanations in (1), but only represents a minimum.

According to Art. 9(2)(a) P2BR, the platform provider must set out its own access to data provided or generated by the business user or the consumer in the GTC. It must explain to which category this data belongs and under which conditions it has access.

According to Art. 9(2)(b) P2BR, the same obligation applies to business users' access to the data that they themselves provide or generate through the use of the platform. Art. 9(2)(c) P2BR also supplements this obligation with data that can be traced back to other business users or consumers.

Article 9(2)(d) of the P2BR also refers to the same obligation with regard to the provision of data to third parties. This concerns both whether data is made available to third parties and whether this is necessary for the online intermediary service. The purpose of the disclosure should also be disclosed. In addition, information should be listed on whether and how the commercial user can object to the transmission of data.[2104]

According to Art. 9(3) P2BR, the information obligations from the first two paragraphs stand independently alongside other EU data protection requirements, in this case the GDPR, Directive (EU) 2016/680 and Directive 2002/58/EC, but must be harmonised with them.[2105]

gg) Restriction on the possibility of introducing other conditions by other means Art. 10 P2BR

According to Art. 10(1) P2BR, platform providers must justify in their general terms and conditions why they prohibit commercial users from offering the same goods or services by other means and under different conditions. Platforms regularly use this sales restriction to prevent the offer on other platforms

2099 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 9 para. 65.
2100 Through Art. 9(3) P2BR reference to Art. 4 No. 1 GDPR, Tribess, H., *ZD* 2020, 440 (442).
2101 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 9 para. 7.
2102 Rec. 33 Regulation (EU) 2019/1150.
2103 Rec. 35 Regulation (EU) 2019/1150.
2104 Rec. 34 Regulation (EU) 2019/1150.
2105 Rec. 35 Regulation (EU) 2019/1150.

or in direct sales at better conditions and thus to bind consumers to their own platform.[2106] Article 10(1) P2BR applies to all prohibitions, requirements or other stipulations regarding other offers to consumers (i.e. offers to traders are not included).[2107] Other conditions can be a different price, other contractual conditions or modified service content.[2108] It does not matter whether the conditions are better or worse for other offers.[2109]

A special feature in contrast to other transparency obligations of the P2BR is that the information from Art. 10 P2BR must both be set out in the GTC and be easily accessible to **the public**, Art. 10(1) P2BR. The information on a restriction must not only be provided, but also justified, Art. 10(1) P2BR.

hh) Internal complaints management, Art. 11 P2BR

(4) Regulatory objective

Art. 11(1) P2BR obliges providers of online intermediary services to set up an internal complaints management system for complaints from business users. The aim of this provision is to provide business users with access to an immediate, appropriate and effective redress system and to create a bilateral, rapid dispute resolution system.[2110] Platform operators, on the other hand, are to be given sufficient flexibility in dealing with complaints and the opportunity to respond appropriately to abusive use of the complaints system.[2111]

It is important to note that according to Art. 11(5) P2BR, the establishment of a complaints management system does not apply to SMEs, but they can set this up voluntarily.

Internal complaint management is the first of three legal protection options available to the user. The second stage is out-of-court mediation (Art. 12 and 13 P2BR) and finally judicial enforcement in accordance with Art. 14 P2BR, whereby the business user is free to choose between the stages and does not have to go through all of them.[2112]

(2) Specifications

According to Article 11(1)(1) of the P2BR, complaints management must have an internal character, i.e. it must be within the sphere of the intermediary service and be carried out either by the platform operator itself or by a third party that complies with the requirements of the P2BR.[2113]

The complaints management system must be easily accessible and free of charge and ensure that complaints are dealt with within a reasonable period of time, Art. 11(1) P2BR. According to Art. 11(2)

2106 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 10 para. 1.
2107 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 10 para. 5a.
2108 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 10 para. 7.
2109 Busch, C./Höppner, T./Wick, J., P2B-VO, 1st ed. 2022, Art. 10 para. 12.
2110 Rec. 37 Regulation (EU) 2019/1150.
2111 Rec. 38 Regulation (EU) 2019/1150.
2112 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 11 para. 11.
2113 Rec. 39 Regulation (EU) 2019/1150.

P2BR, information on the organisation of the complaints procedure and the individual steps, such as examination, processing and clear and comprehensible results of the procedure, must also be recorded.

A distinction must be made between the obligation to include this information in the general terms and conditions in accordance with Art. 11(3) P2BR and the additional obligation to provide information in accordance with Art. 11(4) P2BR on how complaints management works in practice.[2114] According to Art. 11(4) P2BR, information on the number of complaints, the most important types of complaints, the average time required and the outcome must be made easily available to the public.

(3) Demarcation

Art. 20 DSA also requires the establishment of an internal complaints management system, meaning that this obligation arises from both regulations. However, it is important for commercial users that in the event of problems or breaches of the P2B requirements, they can only refer to the complaints management system set up under Art. 11 P2BR and not to a potentially more favourable system under the DSA.[2115]

ii) Duty to mediate, Art. 12 P2BR

Mediation is listed as a further dispute resolution instrument in Art. 12(1) P2BR. The aim of the regulation is to spare the parties lengthy and costly court proceedings.[2116] According to (1), two or more mediators within the meaning of Art. 3(b) of the Mediation Directive[2117] are to be specified by mediation platform providers with whom disputes are to be resolved. Participation in mediation is voluntary for both parties and can be interrupted at any time.[2118]

Art. 12(2) P2BR lists the requirements to be met by mediators. They must be impartial and independent (a), offer affordable services in the language of the GTC without delay (b), (c), (e), be easy to contact (d) and understand the business relationship sufficiently (f).

According to Art. 13 P2BR, mediation organisations can also be appointed. The advantage of this is that, despite the lack of predictability of the commercial user, the mediator has not yet been determined in person and a neutral organisation is therefore selected.[2119] This strengthens trust in mediation.[2120]

b) Online search engines

The P2BR contains far fewer provisions for online search engine operators. They are only mentioned in Art. 5 and 7 of the P2BR.

2114 Köhler, H./ Bornkamm, J/Feddersen, C./Alexander, C., P2B-VO, 14th ed. 2024, Art. 11 para. 33.
2115 Busch, C., *ZdiW* 2021, 88 (91).
2116 Rec. 40 Regulation (EU) 2019/1150.
2117 Directive (EU) 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters, OJ L 136, 24.5.2008, p. 3.
2118 Rec. 40 Regulation (EU) 2019/1150.
2119 Metzger, A./Vetter, S./Witte, Z., *CR* 2020, 739 (742) para. 18.
2120 Metzger, A./Vetter, S./Witte, Z., *CR* 2020, 739 (742) para. 18.

aa) Ranking, Art. 5 P2BR

Art. 5(2) P2BR stipulates that online search engines must also disclose information about their ranking methods. In the absence of a contractual relationship between the provider and the commercial user[2121], there are no general terms and conditions, meaning that online search engines must make the main parameters publicly and easily available in explanatory notes.[2122] It must also be ensured that these are always kept up to date, Art. 5(2)P2BR.

According to Art. 5(4) P2BR, providers of online search engines must notify the user with the company's website of changes due to third-party notifications. This primarily refers to cases in which a company attempts to worsen the ranking of a competitor through notifications such as trademark and copyright infringements.[2123]

In addition, online search engines are required under Article 5(5)(c) of the P2BR to disclose the design characteristics of the website of users with a company website and how these influence the ranking mechanism. Paragraphs 3, 6 and 7 apply accordingly.

bb) Differentiated treatment, Art. 7 P2BR

Parallel to Art. 5(2) P2BR, Art. 7(2) P2BR regulates the obligation to provide information on differentiated treatment for online search engines. In the absence of a comparable provision to Art. 7(1) P2BR, the provider of an online search engine can significantly reduce its explanations. This is due to the fact that the lack of a contractual relationship between an online search engine and a commercial user means that there is less contractual abuse of power.[2124] In contrast to Art. 5(2) P2BR, no precise requirements for the publication of the transparency requirements are standardised. Recital 31 also differs in its wording from that of recital 26 and only requires disclosure in an explanation, but does not mention how this explanation is to be written. There is therefore no clear regulation on how the online search engine operator must provide the explanations. In order to fulfil the purpose of the transparency requirements, the explanations must be made publicly accessible in any case.[2125]

4. Enforcement and supervision

The P2BR does not contain any enforcement instruments of its own, but refers to national (already existing) enforcement mechanisms.[2126] In the absence of its own provisions on fines or the obligation for Member States to enforce the Regulation ex officio,[2127] the P2BR is mainly aimed at civil liability of online platforms in the event of infringements of the P2BR.

2121 See under 2. b) bb).
2122 See also Rec. 26 Regulation (EU) 2019/1150.
2123 Busch, C., P2B-VO, 1st ed. 2022, Art. 5 para. 60.
2124 Busch, C./Podzun, R., P2B-VO, 1st ed. 2022, Art. 7 para. 34.
2125 Steinrötter, B./Louven, S., Europäische Plattformregulierung, 1st ed. 2023, § 17 para. 110.
2126 Busch, C./Höppner, T./Wick, J., P2B-VO, 1st ed. 2022, Art. 15 para. 1.
2127 Rec. 46 Regulation (EU) 2019/1150.

a) Civil liability

aa) Claims under national law, Art. 15 P2BR

The P2BR does not contain any separate bases for claims, meaning that these must be established in national law by the legislator in accordance with Art. 15 P2BR.[2128] The applicable law is determined by private international law. Claims for removal and injunctive relief as well as compensation for damages against online intermediary services can be considered under fair trading law, contract law and tort law. In the absence of a contractual relationship between users and online search engines, contractual claims do not apply here.[2129] Breaches of the provisions of the P2BR may then constitute breaches of duty under national law.[2130] Furthermore, the provisions of the P2BR can be used as judgements in national law.[2131]

bb) Filing a complaint, Art. 14 P2BR

In addition to internal complaints management and mediation, the third level of legal protection options is going to court (private enforcement). Art. 14 P2BR provides an option for legal action, which distinguishes between collective rights in Art. 14(1) P2BR and individual rights in Art. 14(9) P2BR.

Art. 14(1) P2BR opens up the possibility of setting up organisations, associations and qualified public bodies that collectively represent the rights of business users through a **representative action.** The background to the possibility of collective action is the risk that commercial users will not enforce their rights due to a lack of financial resources, fear of retaliation and exclusive provisions of the applicable law on general terms and conditions.[2132] The bodies to be set up must be properly established in accordance with the law of a Member State, must be non-profit organisations and must pursue their objectives on a permanent basis.[2133] This is to ensure that they fulfil their tasks effectively and appropriately and that ad hoc foundations and influences from third-party funds are avoided.[2134] They must also disclose their membership and sources of funding to national courts in order to prevent the associations from being influenced by online platforms.[2135]

In addition, Art. 14(9) P2BR stipulates that commercial users can independently enforce their rights under national law before the national courts. However, Art. 14(9) P2BR only has a clarifying function. The P2BR does not grant a separate individual right of action in addition to national law, but merely stipulates that individual actions under national law are not excluded by Art. 14(1) P2BR.[2136]

2128 Tribess, H., *GWR* 2020, 233 (237).
2129 Steinrötter, B./Tribess, A., Europäische Plattformregulierung, 1st ed. 2023, § 18 para. 76.
2130 District Court Munich I (LG), 5 Sep. 2021 - 37 O 32/21 = MMR 2021, 995, 998.
2131 District Court Munich I (LG), 5 Sep. 2021 - 37 O 32/21 = MMR 2021, 995, 998.
2132 Rec. 44 Regulation (EU) 2019/1150.
2133 Rec. 44 Regulation (EU) 2019/1150.
2134 Rec. 44 Regulation (EU) 2019/1150.
2135 Rec. 44 Regulation (EU) 2019/1150.
2136 District Court Stuttgart (AG), 22 Apr. 2021 - 11 O 10/21 = MMR 2021, 1000, 1004 with reference to Schneider, R./Kremer, F., *WPR* 2020, 1128 (1128).

b) Supervision, Art. 15 P2BR

Pursuant to Art. 15(1) P2BR, the Member States are obliged to enforce the Regulation appropriately and effectively. To this end, effective, proportionate and dissuasive measures must be adopted.[2137] In doing so, they can create new enforcement bodies or utilise existing bodies such as authorities or courts.[2138] According to Art. 15(2) P2BR, the Member States must also adopt provisions on measures in the event of infringements, but are not obliged to take official action against infringements and impose fines.[2139]

c) Example Germany

In Germany, both the P2BR and the DSA are implemented by the Digital Services Act (DDG) of 6 May 2024. The Federal Network Agency is responsible for implementing the P2BR in accordance with § 22(1) DDG. In doing so, it can designate organisations, associations and public bodies in accordance with Art. 14 P2BR, § 22(2) DDG. In addition, it shall cooperate with the Federal Cartel Office in accordance with § 22(3) DDG so that both bodies can fulfil their tasks. According to § 33(3) DDG, the Federal Network Agency can levy fines against online platforms in the event of violations of the provisions of the P2BR.

5. Summary and implications for practice

For the first time, the P2BR creates concrete, harmonised transparency requirements for online platforms. For a regulation to be effective, the addressees must observe the requirements and incorporate them into their activities. In addition, there must be sufficient enforcement options to sanction violations appropriately.

To review this, the EU Commission evaluates the developments of the regulation at regular intervals in accordance with Art. 18 P2BR. It did so most recently in its report dated 12 September 2023.[2140] In this report, the Commission stated that the P2BR does have an impact in terms of transparency requirements, but that its potential is not sufficiently utilised due to a lack of knowledge and implementation of the Regulation.[2141]

The Commission's assessment is based on a survey conducted in 2020, in which 179 online intermediation services were analysed and business users were interviewed.[2142] The findings included the following:

- Only a third of the online platforms list information about ranking parameters in their terms and conditions,[2143] some of which were insufficient to provide clarity for commercial users.[2144]

2137 Busch, C./Höppner, T./Wick, J., P2B-VO, 1st ed. 2022, Art. 15 para. 1.
2138 Rec. 46 Regulation (EU) 2019/1150.
2139 Rec. 46 Regulation (EU) 2019/1150.
2140 COM(2023) 525 final.
2141 COM(2023) 525 final p. 1.
2142 Tribess, A., 'P2B-VO Art. 1', in: BeckOK UWG (26th ed. 2024) para. 5b.
2143 COM(2023) 525 final p. 4.
2144 COM(2023) 525 final p. 10 et seq.

- Only 19 of the 179 online platforms analysed have introduced an internal complaints management system. In addition, the number of complaints submitted and reviewed shows that the online platforms define the term complaint inconsistently.[2145]
- Only 25 online platforms name two mediators in their T&Cs in accordance with Art. 12 P2BR. 35 others name one mediator, with most of them naming the same mediator based outside the EU.[2146]
- The establishment of a specialised mediation centre within the meaning of Art. 13 P2BR is not known.[2147]

These results show that the platforms do not fully comply with the regulation in a targeted manner. As a result, commercial users are not or not sufficiently informed about their rights and legal protection options.

In addition, the P2BR does not require administrative enforcement of the P2BR by the Member States. Therefore, if the Member States do not introduce their own system of fines, infringements of the P2BR can generally only be enforced by way of private enforcement.[2148] In the absence of sufficient information about a complaints management system in accordance with Art. 11 P2BR and mediation in accordance with Art. 12 P2BR, commercial users hardly ever use these channels.[2149] Business users regularly lack the time and money for individual complaints, and there is also a fear of retaliation by online platforms.[2150] Furthermore, there must be legal standing under national law for an individual action, as Art. 14(9) P2BR does not create such standing. The associations or organisations named in Art. 14 P2BR, which are authorised to bring a representative action, were only established by Ireland and Austria at the time of the Commission's assessment, meaning that many commercial users are also denied the opportunity to bring a representative action. In addition, on 26 January 2023, the Commission filed infringement proceedings against eight Member States that have not created any measures under Art. 15 P2BR.[2151]

These circumstances make it clear that effective legal enforcement in the event of infringements of the P2BR is not guaranteed at the time of the report, but that this is necessary in order for the Regulation to create sufficient transparency. As a first step, the Commission intends to provide more information to business users in order to inform them about their rights and legal protection options. [2152]

2145 COM(2023) 525 final p. 7 et seq.
2146 COM(2023) 525 final p. 9.
2147 COM(2023) 525 final p. 9.
2148 Busch, C./Höppner, T./Wick, J., P2B-VO, 1st ed. 2022, Art. 15 para. 7.
2149 COM(2023) 525 final p. 12.
2150 COM(2023) 525 final p. 12.
2151 COM(2023) 525 final p. 13.
2152 COM(2023) 525 final p. 16.

V. Digital Service Act (DSA) - Regulation (EU) 2022/2065

Bibliography

Apel, S., & Huber, C., "Das neue Datenrecht der EU – Eine Übersicht," JuS (2024), 514; Beaujean, D., Oelke, C., & Wierny, T., "Immer mehr Verordnungen aus Brüssel und ihre Auswirkungen auf die Medienregulierung," *MMR* (2023), 11; Berberich, M., & Seip, F., "Der Entwurf des Digital Services Act," *GRUR-Prax* (2021), 4; Dregelies, M., "Überblick über den Rechtsrahmen für das Internet," *MMR* (2022), 1033; Dregelies, M., "Verbraucherschutz im Digital Services Act," *VuR* (2023), 175; Dreier, T., & Leistner, M., "Urheberrecht im digitalen Binnenmarkt," *GRUR* (2013), 881; European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions – A Digital Single Market Strategy for Europe," COM(2015) 192 final; Gerdemann, S., & Spindler, G., "Das Gesetz über digitale Dienste (DSA) (Teil 1)," *GRUR* (2023), 3; Gerdemann, S., & Spindler, G., "Das Gesetz über digitale Dienste (DSA) (Teil 2)," *GRUR* (2023), 115; Gerpott, T., "Das Gesetz über digitale Dienste nach den Trilog-Verhandlungen," *CR* (2022), 516; Gersdorf, H., & Paal, B. (eds.), Beck'scher Online-Kommentar Informations- und Medienrecht, 44th ed., Status: 1 February 2023, C.H. Beck; Gielen, N., & Uphues, S., "Digital Markets Act und Digital Services Act," *EuZW* (2021), 627; Herdegen, M., Europarecht, 24th ed., C.H. Beck 2023; Hoeren, T., Sieber, U., & Holznagel, B. (eds.), Handbuch Multimedia-Recht, 62nd ed., C.H. Beck 2024; Hofmann, F., & Raue, B. (eds.), Digital Service Act – Gesetz über digitale Dienste, 1st ed., Nomos 2023; Holznagel, D., "Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act," *CR* (2021), 123; Holznagel, D., "Zum Stand des Herkunftslandprinzips der E-Commerce-RL," *CR* (2023), 321; Janal, R., "Haftung und Verantwortung im Entwurf des Digital Services Acts," *ZEuP* (2021), 227; Kaesling, K., "Regulierung von Dark Patterns im Digital Services Act," *NJW* (2024), 1609; Kaesling, K., "Evolution statt Revolution der Plattformregulierung," *ZUM* (2021), 177; Kalbhenn, J., & Hemmert-Halswick, M., "EU-weite Vorgaben für die Content-Moderation in sozialen Netzwerken," *ZUM* (2021), 184; Kraul, T. (ed.), Das neue Recht der digitalen Dienste, Nomos 2023; Laude, L., "DSA-Umsetzung abseits sehr großer Online Plattformen – Zur Konkretisierung unkonkreter Maßstäbe," *RDi* (2024), 216; Legner, S., "Der Digital-Service-Act – Ein neuer Grundstein der Digitalregulierung," *ZUM* (2024), 99; Martini, M., Drews, C., Seeliger, P., & Weinzierl, Q., "Dark Patterns – Phänomenologie und Antworten der Rechtsordnung," *ZfDR* (2021), 47; Müller-Terpitz, R., & Köhler, M., Digital Services Act: DSA – Gesetz über digitale Dienste, Nomos 2024; Podszun, R., Bongartz, P., & Kirk, A., "Digital Markets Act – Neue Regeln für Fairness in der Plattformökonomie," *NJW* (2022), 3249; Raue, B., "Plattformnutzungsverträge im Lichte der gesteigerten Grundrechtsbindung marktstarker sozialer Netze," *NJW* (2022), 209; Raue, B., & Heesen, H., "Der Digital Services Act," *NJW* (2022), 3537; Rössel, M., "Digital Services Act: Haftungsprivilegierungen, Überwachung und Blockadeanordnungen – Sezierung verabschiedeter Änderungen aus dem Trilog in drei Akten – Teil 1," *ITRB* (2023), 12; Schröder, C., & Hardan, O., "Der Digital Services Act ist da – Was sind die Auswirkungen für kleinere und mittelständische Unternehmen?" *BB* (2023), 579; Schweitzer, H., "Digitale Plattformen als private Gesetzgeber: Ein Perspektivwechsel für die europäische ‚Plattform-Regulierung'," *ZEuP* (2019), 1; Sesing-Wagenpfeil, A., "Der ‚barmherzige Samariter' im DSA," *MMR* (2023), 655; Sesing-Wagenpfeil, A., "Suchmaschinen im Digital Services Act," *CR* (2023), 113; Spindler, G., "Der Vorschlag für ein neues Haftungssystem für Internetprovider – der EU-Digital-Service-Act (Teil 1)," *GRUR* (2021), 545; Spindler, G., "Löschung und Sperrung von Inhalten aufgrund von Teilnahmebedingungen sozialer Netzwerke," *CR* (2019), 238–246; Spindler, G., & Schmitz, P. (eds.), Telemediengesetz, 2nd ed., C.H. Beck 2018.

1. Introduction

The Digital Services Act (hereinafter: DSA) is a globally unprecedented step towards regulating intermediary services and online platforms in particular.[2153] Thus, the European legislator has created a regulatory system with specific liability rules and special due diligence obligations for online intermediary services, which came into force on 17 February 2024. With its 156 recitals and 93 articles, the DSA sets out a comprehensive regulatory concept, which is presented below.

a) Background and relationship to the E-Commerce Directive, Art. 2, 89 DSA

The DSA follows on directly from its predecessor, the E-Commerce Directive 2000/31/EC[2154].[2155] According to recital 16 of the DSA, the DSA recognises the progress made by the E-Commerce Directive towards legal certainty; the DSA therefore has no effect on the application of the Directive, Art. 2(3) DSA. Excluded from this are the liability privileges provided for by the E-Commerce Directive in Art. 12 to 15, which are deleted in accordance with Art. 89(1) DSA – they find their successor provisions in Art. 4–6, 8 DSA, which largely correspond to the content of the predecessor provisions and merely provide for clarifications. Art. 89(2) DSA also stipulates that references to Art. 12 to 15 of the E-Commerce Directive are to be understood as references to Art. 4–6 DSA and Art. 8 of the DSA. It can be deduced from the coexistence of the regulatory systems that the revision of the liability provisions of the E-Commerce Directive as the "cornerstone of the internet economy"[2156] was not intended to be a fundamental overhaul, but rather the creation of a regulatory framework that is directly binding in all Member States. The main difference between the E-Commerce Directive and the DSA is therefore not of a substantive nature, but merely of a technical legal nature: While the DSA, as a regulation within the meaning of Art. 288(2) TFEU, is binding in all Member States, the E-Commerce Directive first had to be implemented by the Member States and was therefore susceptible to national specificities (Art. 288(3) TFEU).[2157] If the teleological considerations of the DSA and the E-Commerce Directive are mirrored, it is also noticeable that the DSA provides for an extension of the intended objectives.[2158] Article 1(1) of the E-Commerce Directive is still limited to contributing to the proper functioning of the internal market by ensuring the free movement of information society services between Member States. According to Art. 1(1) DSA, the DSA expands its thrust to the effect that even before the functioning of the internal market, the security, predictability and trustworthiness of the online environment, the promotion of innovation and the fundamental rights of the EU Charter are cited. In this respect, it must be recognised

2153 Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (124).

2154 Directive (EU) 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), OJ L 178 of 17 July 2000, p. 1-16, hereinafter E-Commerce Directive.

2155 Legner, S., *ZUM* 2024, 99 (100); Dregelies, M., *MMR* 2022, 1033 (1033).

2156 Berberich, M./Seip, F., *GRUR-Prax* 2021, 4 (6).

2157 Herdegen, M., Europarecht, 24th ed. 2023, § 8 Part 2 IV para. 61, 62.

2158 Steinrötter, B, Europäische Plattformregulierung, 1st ed. 2023, § 1 para. 7.

that the DSA has outgrown the regulatory objectives of the E-Commerce Directive in view of the fundamental changes in the information society.

b) Legal policy considerations

More than two decades after the E-Commerce Directive, a fundamental change in the internet economy can be recognised: Information Society services have become an integral part of the daily lives of EU citizens.[2159] The DSA thus emphasises the relevance of information society services right from the start. The DSA is committed to finding a balance between restriction and freedom; online platforms are not to be called into question entirely.[2160] Rather, the desired status quo is that the risks and challenges associated with them should be addressed and thus tackled "for each individual user of the respective service, the companies and society as a whole"[2161]. This need results from the downsides of the increased relevance of internet services.

A core concern of the DSA is the legal containment of disinformation and hate speech.[2162] Although these are not genuine problems of the internet, the ubiquitous nature of the internet creates an extremely suitable breeding ground.[2163] The high speed of data processing and dissemination and the anonymity of the Internet are just two factors that promote the easy spread of disinformation.[2164] The danger of disinformation is further increased by the fact that people are increasingly obtaining their information exclusively via social networks and, as a result, online platforms have ever greater power of opinion and, in extreme cases, can be used by governments as a "propaganda weapon".[2165] As the currency of the internet, user numbers and user dwell time have an influence on the fact that the most "adventurous"[2166] statements, i.e. hate speech in particular, can generate a lot of attention.[2167] As a result, social media is like a megaphone, especially for extreme opinions.[2168]

The increased influence of digital services has also created a power imbalance - on the one side are the major media services, on the other are the remaining commercial players, consumers and state authorities. [2169] Online platforms have long ceased to be "extremely delicate and nurturing little plants".[2170] The services decide de facto independently on the "whether" to grant access and the "how" of permissible

2159 Rec. 1 Regulation (EU) 2022/2065.
2160 Steinrötter, B, Europäische Plattformregulierung, 1st ed. 2023, § 1 para. 8.
2161 Rec. 1 Regulation (EU) 2022/2065.
2162 Rec. 9, 12 Regulation (EU) 2022/2065.
2163 Legner, S., *ZUM* 2024, 99 (100).
2164 Steinbach, M./Bader, K, Disinformation aufdecken und bekämpfen, 1st ed. 2020, p. 15, 22 et seq.
2165 Gielen, N./Uphues, S., *EuZW* 2021, 627 (632).
2166 Gielen, N./Uphues, S., *EuZW* 2021, 627 (632).
2167 Gerpott, T., *CR* 2022, 516 (517) para. 2.
2168 Gielen, N./Uphues, S., *EuZW* 2021, 627 (632).
2169 Kraul, T., Das neue Recht der Plattformregulierung, 1st ed. 2023, § 2 para. 2; Legner, S., *ZUM* 2024, 99 (100).
2170 Dreier, T./Leistner, M., *GRUR* 2013, 881 (881).

behaviour; they have become "private legislators".[2171] To put it bluntly, the relationship between platform and consumer can be compared to a "do-or-die situation".[2172] The power of internet services, which the DSA is committed to containing, is vividly illustrated by the consequences of the storming of the Capitol in 2021, when ‘Twitter‘, ‘Facebook‘ and ‘YouTube‘ subsequently blocked Donald Trump's accounts. The most powerful man in the world at the time was robbed of one of his most important communication media by the power of internet services.[2173]

In response to this demonstration of power, EU Commissioner ‘Thierry Breton‘ proclaimed: "Just as 11 September marked a paradigm shift in global security policy, 20 years later we have witnessed a before and after in the role of digital platforms in our democracy."[2174] The DSA is therefore a step by the EU Commission towards creating "a Europe for the digital age"[2175].

c) Concrete goals

According to Art. 1(1) DSA, the aim of the DSA is to create a safe, predictable and trustworthy online environment in which innovation is encouraged and the fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected. In line with the above legal policy considerations, the DSA is intended to provide an appropriate counterbalance to the power of large internet platform operators and to regulate competition and illegal content.[2176] In addition, the recitals can be consulted for more detailed background information.

The premise prior to the adoption of the DSA was that the Member States primarily issued national regulations. This resulted in a fragmented internal market,[2177] which is particularly problematic given the cross-border nature of the internet.[2178] In France, for example, the ‘Loi Avia‘[2179] (anti-hate law) came into force in 2020, but was classified as partially unconstitutional just one month later.[2180] The NetzDG was enacted at German level.[2181] The background to these national efforts was that the E-Commerce Directive was no longer considered sufficient to contain the risks and challenges of the internet.[2182] In addition to the positive effects of the prevailing platform economy on the Internet, numerous negative

2171 Schweitzer, H., *ZEuP* 2019, 1 (1).
2172 Podszun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3249).
2173 Conger, K./Isaac, M./Frenkel, S., Twitter and Facebook Lock Trump's Accounts After Violence on Capitol Hill, New York, https://www.nytimes.com/2021/01/06/technology/capitol-twitter-facebook-trump.html (last accessed on 1 November 2024).
2174 Breton, T., The Storm on Capital Hill is a Digital "9/11" Moment, https://www.welt.de/debatte/article225006167/Thierry-Breton-Der-Sturm-auf-Capitol-Hill-ist-ein-digitaler-9-11-Moment.html (last accessed 1 November 2024).
2175 COM/2015/192 final.
2176 Gielen, N./Uphues, S., *EuZW* 2021, 627 (627).
2177 Rec. 2 Regulation (EU) 2022/2065; BT Wissenschaftliche Dienste No. 10/20 of 15 Sep. 2020, p. 1.
2178 Rec. 2 Regulation (EU) 2022/2065.
2179 Conseil constitutionnel Décision n° 2020-801 DC of 18 June 2020.
2180 Dregelies, M., *MMR* 2022, 1033 (1033).
2181 Act amending the Network Enforcement Act of 3 June 2021 (Federal Law Gazette I p. 1436).
2182 Steinrötter, B, Europäische Plattformregulierung, 1st ed. 2023, § 1 para. 9.

effects have also emerged: for example, the positive network effects promoted on the one hand,[2183] on the other, can lead to market concentration. Other examples include criminal offences that are difficult to prosecute, threats to informational self-determination, copyright infringements and the increase in hate, hate speech and fake news on the internet.[2184] These efforts by member states to adopt national regulations were also fuelled by the fact that the European Union had previously been reluctant to adopt its own regulations in this area and that these codes of conduct[2185] and recommendations[2186] were all rather vague and non-binding.[2187] As a result, there was a growing need to take account of the new risks that had emerged.[2188] The European legislator responded to this need and standardised the law with the DSA. The rules adopted in the form of a Regulation will be directly applicable in the EU. The European Commission hopes that this will give companies access to new markets and opportunities to utilise the benefits of the internal market, while at the same time offering consumers and other users greater choice.[2189]

In addition, the DSA aims to ensure effective protection of fundamental rights in the digital sector by creating an environment that guarantees European (fundamental) rights such as freedom of expression and information (Art. 11 CFR) to the greatest possible extent.[2190] In the long term, the legal certainty thus created should mean that innovation is no longer hindered, but rather encouraged, and at the same time promote interoperability, i.e. the interaction of different intermediary services.[2191]

In addition to the predominantly economic considerations, democratic and socially relevant concerns were also at the forefront when the DSA was adopted.[2192] This can be seen, for example, in recital 40 of the DSA, which stipulates that the established due diligence obligations are also intended to achieve political objectives such as the security and trust of the user. As recital 9 of the DSA shows, the aim is to achieve a standardised, secure, predictable and trustworthy online environment.

d) Basic structure

In terms of content, the DSA provides in particular for liability rules and **due diligence obligations** for intermediary services and procedural enforcement mechanisms, Art. 1(2) DSA. In Chapter I, the DSA first defines general provisions and thus draws general definitions "in front of the bracket".[2193] The focus

---

2183 On network effects Hoeren, T. /Sieber, U./Holznagel, B. /Beckmann, K./Müller, U., Handbuch Multimedia-Recht, Teil 10 Kartellrecht, para.186.

2184 Dregelies, M., *MMR* 2022, 1033 (1033); Gielen, N./Uphues, S., *EuZW* 2021, 627 (632).

2185 For example, Code of Conduct on Countering Illegal Hate Speech Online and EU Code of Practice on Disinformation.

2186 For example, Commission Recommendation (EU) 2018/334 of 1 March 2018 on effective measures to tackle illegal content online, OJ L 63/50 of 6 March 2018, p. 50 - 61.

2187 Gielen, N./Uphues, S., *EuZW* 2021, 627 (632).

2188 Steinrötter, B, Europäische Plattformregulierung, 1st ed. 2023, § 1 para. 9.

2189 Rec. 2 Regulation (EU) 2022/2065.

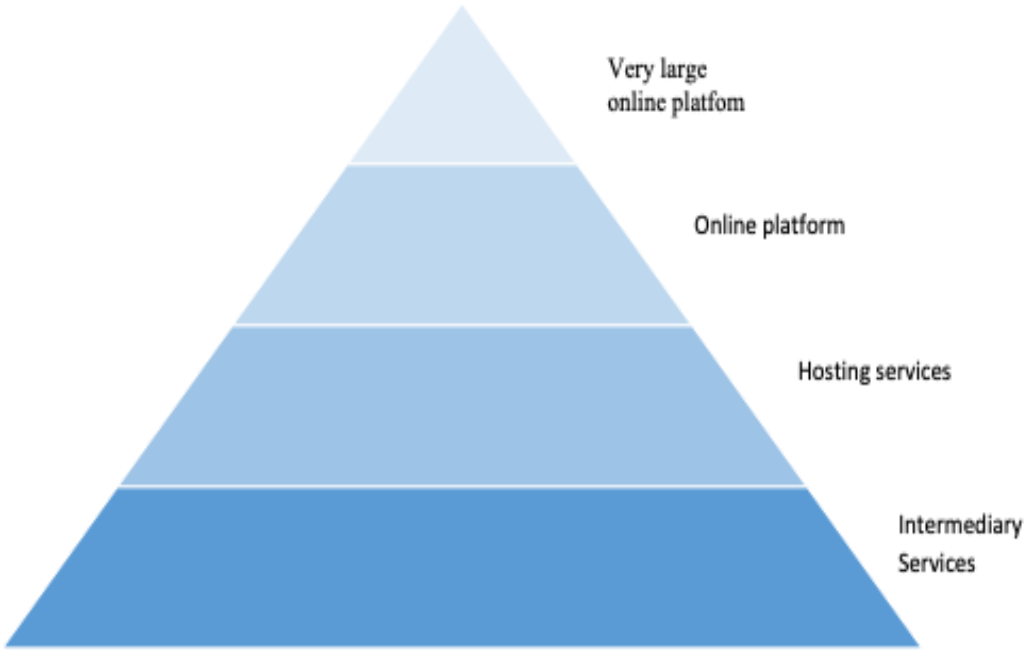
2190 Rec. 3 Regulation (EU) 2022/2065.

2191 Rec. 4 Regulation (EU) 2022/2065.

2192 Steinrötter, B., Europäische Plattformregulierung, 1st ed. 2023, § 1 para. 11; *Beaujean/Oelke/Wierny,* MMR 2023, 11, 12.

2193 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 3 para. 1.

of the DSA is on the envisaged **liability privileges** (Chapter II) and due diligence and transparency obligations (Chapter III). Structurally, the DSA follows a **system of tiered liability**.[2194] Within this tiered system, internet services are divided into four categories. Each additional category represents a subset of the previous one. Starting with intermediary services as the addressees of the standard, Chapters II and III § 1 provide for general regulations. The further regulatory levels are aimed at individual providers of intermediary services and provide for supplementary requirements. This creates a basic structure that provides for increasing regulatory intensity for an ever smaller subset of norm addressees that are categorised as more risky.[2195] The result is a "pyramid **model**" based on gradual liability :[2196]



Source: Own illustration

The tiered regulatory system is partially continued in the subsequent provisions of the fourth chapter. This chapter contains the supervisory and enforcement mechanisms of the regulation.

2. Area

a) Material-personal scope

The central concept of the DSA is that of an **intermediary service**.[2197] According to Art. 1(2) DSA, the DSA is a legal framework for the provision of services. The material scope of the DSA is therefore determined by the term "intermediary service" within the meaning of Art. 3(g) DSA.[2198]

2194 Gerdemann, S./Spindler, G., *GRUR* 2023, 3 (3).
2195 Gerdemann, S./Spindler, G., *GRUR* 2023, 3 (3).
2196 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Introductory marginal No. 4.
2197 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 3 para. 40.
2198 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 3 para. 40.

aa) Intermediary services, Art. 3(g) DSA

Art. 3(g) DSA defines the intermediary service as one of the listed information society services. The term "intermediary service" thus refers primarily to the activity carried out by the service. The listed information society services include

- (i) the **mere conduit,** which consists of transmitting information provided by a user in a communications network or providing access to a communications network;
- (ii) a **caching** service, which consists of transmitting information provided by a user in a communication network, whereby an automatic, time-limited intermediate storage of this information takes place for the sole purpose of making the transmission of the information to other users more efficient at their request;
- (iii) a **hosting** service, which consists of storing information provided by a user on the user's behalf.

The basic requirement is that it is an **information society service**. This is defined in Art. 3(a) DSA, which in turn refers to Art. 1(1)(b) of the Info Directive[2199].[2200]

The common feature of all intermediary services mentioned in Art. 3(g) DSA is that the activity they provide is linked to the provision of information by the user; all intermediary services therefore take on the role of an **intermediary**.[2201]

bb) Individual intermediary services, Art. 3(g)(i)–(iii) DSA

As explained above, the DSA follows the principle of tiered regulation, i.e. the scope covers different norm addressees depending on the tier.[2202] These are differentiated according to the type of service they provide:

(5) Pure transit, Art. 3(g)(i) DSA

Art. 3(g)(i) DSA covers switching services whose service consists **purely of routing** (Art. 4(1) DSA). The provisions apply to services that transmit data packets to the recipient, whereby the intermediary service may not have any influence on the selection or content (**rooting**).[2203] In addition, so-called **access providers**, which provide access to a communications network,[2204] also fall within the scope .

Recital 29 mentions, for example, Internet exchange nodes, wireless access points, virtual private networks (VPN), DNS services and DNS resolvers.

2199 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services, OJ L 241, 17.9.2015, p. 1 - 15.

2200 For the term information society service within the meaning of the Info Directive, see B. I. 2. b) aa) (1) (b).

2201 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 3 para. 45.

2202 Steinrötter, B./Schauer, L., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 19.

2203 For § 8(1) TMG see Spindler, G./Schuster, F./Hoffmann, H./Volkmann, C., 4th ed. 2019, TMG § 8 para. 16.

2204 For § 8(1) TMG see Spindler, G./Schuster, F./Hoffmann, H./Volkmann, C., 4th ed. 2019, TMG § 8 para. 17.

Internet exchange points, also known as Internet Exchanges (IX), are physical infrastructures that enable various network operators to exchange data directly and thus increase the efficiency of data traffic. The best-known providers in Germany include DE-CIX, AMS-IX and Equinix.[2205] Wireless access points, often referred to as WLAN hotspots, are devices that allow users to access the internet wirelessly by connecting to an existing network. Providers of such services include telecommunications companies such as Deutsche Telekom and Vodafone, which provide public Wi-Fi networks.[2206] Interpersonal communication services also fall into the group of pure routing. Examples include Zoom and Skype.[2207]

According to Art. 4(2) DSA, automatic, short-term intermediate storage is also included in addition to pure transmission.

(2) Caching service, Art. 3(g)(ii) DSA

Caching is the temporary intermediate storage of information.[2208] According to Art. 3(g)(ii), 5(1) DSA, the performance of a caching service is to be seen in the fact that the switching service transmits the information provided by a user in a communication network, whereby an automatic, time-limited intermediate storage of this information takes place for the sole purpose of making the transmission of the information to other users more efficient at their request. According to recital 29, this includes the sole operation of networks for the provision of content, 'reverse proxies' or 'proxies' for the customisation of content.

Content customisation 'proxies' are services that filter or modify data traffic in order to adapt certain content to the needs of users or to enable or restrict access to certain information. Providers of such 'proxies include content delivery networks' (CDNs) such as 'Cloudflare' or 'Akamai', which optimise and provide content, as well as specialised filter solutions that are used in schools or companies.[2209] 'Reverse proxies' include 'Cloudflare and 'NGINX', which offer both security and load balancing to optimise the performance of websites. 'Reverse proxies' are aimed at various customer segments, including large companies that want to secure and optimise their web applications, as well as e-commerce platforms that require high availability and fast loading times. Smaller companies and start-ups also use 'reverse proxies' to reduce the load on their IT infrastructure and integrate security solutions. This technology is fundamentally relevant for anyone looking for an improved user experience and robust security measures.[2210]

2205 Federal Network Agency, Study on the implementation of the DSA in Germany, 2024, p. 24.
2206 Federal Network Agency, Study on the implementation of the DSA in Germany, 2024, p. 25.
2207 Federal Network Agency, Study on the implementation of the DSA in Germany, 2024, p. 31.
2208 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 5 para. 13.
2209 Federal Network Agency, Study on the implementation of the DSA in Germany, 2024, p. 40 et seq.
2210 Federal Network Agency, Study on the implementation of the DSA in Germany, 2024, p. 42.

The caching service must be differentiated in two respects: Firstly, it must go beyond mere transmission, as otherwise it would be a mere conduit. Secondly, permanent storage would be a case of a hosting service.[2211]

(3) Hosting service, Art. 3(g)(iii) DSA

Art. 3(g)(iii), Art. 6(1) DSA addresses such intermediary services that provide hosting services. A hosting service consists of storing the information provided by a user on their behalf.[2212]

Cloud computing services are a particularly good example of this.[2213] Cloud computing services offer IT resources such as computing power, storage and networks via the internet, which can be used flexibly as required. They are offered in various models, including 'Infrastructure-as-a-Service', 'Platform-as-a-Service' and 'Software-as-a-Service'. The most important providers include leading global companies such as 'Amazon Web Services', 'Microsoft Azure' and 'Google Cloud'.[2214] Web hosting services also fall into the category of hosting services. These make it possible to provide websites and applications on external servers that are managed by specialised providers. Well-known providers include companies such as 'IONOS', 'Strato' and 'Hetzner'.[2215]

A sub-category of hosting services are **online platforms**, which in turn are subject to separate regulations.[2216] Online platforms are used to store information entered by users, which is disseminated publicly. The business models include social networks, content sharing platforms, music streaming platforms and video streaming platforms. This includes large providers such as 'Facebook', 'Spotify' and 'YouTube'.[2217]

cc) Online search engine as intermediary services, Art. 3(j) DSA

Online search engines are a special category of intermediary services. The online search engine is defined in Art. 3(j) DSA: It is a mediation service that enables users to enter queries in order to search on any topic on any website and receive results in any format.

However, the legal definition of online search engines is contradicted by Art. 2(1) DSA, according to which the regulation applies to intermediary services offered to users with a place of establishment or registered office in the Union [...]. In contrast, Art. 3(g) DSA does not list online search engines as intermediary services. If Art. 3(g) DSA is to be understood as exhaustive,[2218] the categorisation of online search engines as intermediary services within the meaning of the DSA cannot at least be derived from

---

2211 Steinrötter, B./Conrad, A., Europäische Plattformregulierung, 1st ed. 2023, § 3 para. 120.
2212 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 3 para. 60.
2213 Rec. 29 of Regulation (EU) 2022/2065.
2214 *Federal Network Agency*, Study on the implementation of the DSA in Germany, 2024, p. 54 et seq.
2215 *Federal Network Agency*, Study on the implementation of the DSA in Germany, 2024, p. 55 et seq.
2216 Laude, L., *RDi* 2024, 216, 219 et seq. on online platforms.
2217 *Federal Network Agency*, Study on the implementation of the DSA in Germany, 2024, p. 73 et seqq.
2218 Rössel, M., *ITRB* 2023, 12, 13 et seq.; Sesing-Wagenpfeil, A., *CR* 2023, 113, 118; Dregelies, M., *MMR* 2022, 1033 (1034); Raue, B./Heesen, H., *NJW* 2022, 3537, 3538.

Art. 3(g) DSA. Meanwhile, the wording of Art. 3(j) DSA expressly provides that online search engines are intermediary services.[2219] Opinions differ as to how this conflict should be resolved:

One possibility would be to categorise the online search engine in the intermediary triad.[2220] In favour of this, it is argued that numerous provisions explicitly refer to the online search engine as an intermediary service; in particular the exclusion of general monitoring obligations in Art. 8 DSA and the provisions of Art. 11–15 DSA that apply to all intermediary services.[2221] It can therefore be assumed that the omission from the list in Art. 3(g) DSA does not constitute a drafting error.[2222] In this respect, it would then be deliberately left to the user of the law to subsume the online search engine under one of the categories. However, if this view is accepted, it remains unclear under which category the online search engines should be placed.[2223] With reference to the ECJ, which has tended towards such a categorisation,[2224] it could be assumed that online search engines are hosting providers.[2225] This is supported by the fact that this would explain Art. 35(1) DSA, which seems to assume in (g) that online platforms belong to the sub-category of hosting services. An argument against such a categorisation is that the online search engine is always mentioned alongside the online platform, i.e. it would be contradictory to subsume it under the umbrella category.[2226] Online search engines also do not fit under the definition of a hosting service, as they do not carry out indexing on behalf of the user. To resolve the conflict, only the assumption of a de facto order could be considered, so that it is sufficient that the user does not object to the indexing.[2227] It is therefore difficult to resolve the ambiguity by trying to integrate the online search engine into the mediation triad.

Another possibility would be to recognise online search engines as a **fourth category in their own right.** As a consequence, the lack of mention as an independent category would then have to be an editorial error. The consequence of this would be that only those provisions would apply to online search engines that explicitly mention them or that apply to all intermediary services. This is particularly supported by the fact that online platforms are always mentioned alongside another intermediary service and should therefore not be subordinate to it.[2228]

Ultimately, the solution to be supported is to recognise as a first step that online platforms are intermediary services. In a second step, however, they are too heterogeneous to be clearly categorised as one

---

2219 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 3 para. 63.
2220 Dregelies, M., *MMR* 2022, 1033, 1034; Raue, B./Heesen, H., *NJW* 2022, 3537, 3538.
2221 Raue, B./Heesen, H., *NJW* 2022, 3537, 3538.
2222 Raue, B./Heesen, H., *NJW* 2022, 3537, 3538.
2223 On the previous legal situation under the TMG: Higher Regional Court Cologne (OLG Köln), judgment of October, 13, 2016 - 15 U 189/15 = BeckRS 2016, 18916, para. 93; see also Higher Regional Court Celle (OLG Celle), judgement of June 1, 2017 = BeckRS 2017, 124906, para. 13.
2224 Cf. CJEU, 23. Mar. 2010, case C-236/08 to C-238/08, ECLI:EU:C:2010:159 = *NJW* 2010, 2029 para. 110 et seq. - Google France.
2225 Raue, B./Heesen, H., *NJW* 2022, 3537, 3538.
2226 Rössel, M., *ITRB* 2023, 12, 13.
2227 Raue, B./Heesen, H., *NJW* 2022, 3537, 3538.
2228 Raue, B./Heesen, H., *NJW* 2022, 3537, 3538.

type of intermediary service.[2229] However, a fourth category should not be used to resolve this, but the intermediary service should be assessed on the basis of its individual function. This means that each individual duty of care must be analysed separately on the basis of its objective and interests to determine whether it should be applied to the search engine.[2230] Recital 29 DSA also tends in this direction. According to this, the categorisation depends exclusively on its technical functions. The criticism that search engines could not be covered by the DSA is therefore unfounded.[2231] The legislator has left the categorisation of a search engine to a case-by-case assessment.[2232]

b) Territorial scope (market place principle), Art. 2(1) DSA

According to Art. 2(1) DSA, the applicability of the DSA depends on the offer of intermediary services being directed at users with a place of establishment or registered office within the territory of the Union. The DSA thus follows the **market place principle** and is therefore in line with other European legal acts, such as the General Data Protection Regulation (EU) 2016/679 (GDPR).[2233] In this respect, the scope of the DSA also applies to intermediary services that do not have an establishment in the Union but offer their services to users who have a registered office or place of business.[2234] As a result, the scope is considerably broader than it would have been if a country-of-origin principle had been enshrined. As a result, more platforms without an establishment in the Union can be covered.[2235] This is particularly welcome because it can prevent competitive disadvantages and the threat of migration out of the Union.[2236]

It covers users who are resident in a Member State or business users who are established in the Union.[2237] An establishment within the meaning of EU law is the effective exercise of an economic activity by means of a fixed establishment in another Member State for an indefinite period of time.[2238] According to Art. 3(b) DSA, a user is any natural or legal person who uses an intermediary service. Recital 2 DSA clarifies that, in addition to consumers, commercial users are also covered. It should be noted that, according to the case law of the ECJ, only low requirements are placed on establishment and therefore even minor activities are sufficient. [2239]

2229 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 3 para. 60.
2230 Steinrötter, B./Schauer, L., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 54; Dregelies, M., *MMR* 2022, 1033 (1034); Sesing-Wagenpfeil, A., *CR* 2023, 113, 118.
2231 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 5 para. 52.
2232 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 5 para. 51.
2233 Steinrötter, B./Schauer, L., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 62.
2234 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 2 para. 7.
2235 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 2 para. 3.
2236 Bundesrat BR-Drs. 96/21B, 6.
2237 Steinrötter, B./Schauer, L., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 63.
2238 Case law of the CJEU on Art. 49 TFEU; CJEU, 25. July 1991, case C- 221/89 = BeckRS 2004, 75196, para. 20 - Factortame I.
2239 CJEU, 1. Oct. 2015, case C-230/14, ECLI:EU:C:2015:639 = *NJW* 2015, 3636, para. 31 - Weltimmo.

Art. 2(1) DSA is based on whether the intermediary services are offered in the Union. According to Art. 3(d) DSA, this requires that legal and natural persons in one or more Member States are given the opportunity to use the services and that the intermediary service has a substantial connection to the Union. Such a connection exists on the one hand if the service provider is established in the EU. Art. 3(e) DSA mentions, for example, the number of users in the territory of the Union (Art. 3(e), second indent, first indent, DSA) or the specific targeting of Member States (Art. 3(e), second indent, second indent, DSA). With the first criterion in particular, the DSA makes it clear that the application is not necessarily based on the targeting by the provider itself, but is also given if a significant number in relation to the general population of the Member State uses the intermediary service.[2240] According to recital 8 of the DSA, the determination of targeting is based on the circumstances of the specific individual case. The criteria to be applied are the available language, currency or availability in the respective national app store. The DSA is similar to the P2BR and the GDPR in terms of the connecting factor of offering. These also apply when the service is offered in the Union.[2241] It is therefore advisable to interpret the terms coherently.[2242]

On the negative side, Art. 2(2) DSA stipulates that the DSA only applies to intermediary services within the meaning of the Regulation. Although this is logical, Art. 2(2) DSA also explicitly states this once again.[2243]

With the exception of Art. 12–15, the DSA does not affect the provisions of the E-Commerce Directive.[2244] As a result, Art. 3 of the E-Commerce Directive, which lays down the **country of origin principle**, remains in force alongside the provisions of the DSA. This means that each Member State continues to ensure that the information society services provided by a service provider established in its territory comply with the national provisions applicable in that Member State, which fall within the coordinated area[2245].[2246] The law of the country of establishment is decisive for legal responsibility. This means that, with the exception of the provisions of Art. 3(4) of the E-Commerce Directive, the country of origin principle stipulates that the service provider may not be subject to stricter regulations than those of its country of domicile.[2247] With the application of the DSA, this significant limit for the responsibility of service providers has been reduced to the extent that the DSA has a conclusive harmonisation effect.[2248] As a result, national regulations are superseded if and to the extent that the DSA provides for conclusive requirements.[2249]

2240 Steinrötter, B./Schauer, L., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 65.
2241 Art. 1(2) P2BR and Art. 3(2)(a) GDPR.
2242 Dregelies, M., *MMR* 2022, 1033 (1034).
2243 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 2 para. 3.
2244 Art. 2(3) Regulation (EU) 2022/2065.
2245 Legal definition Art. 2(h) E-Commerce Directive.
2246 Art. 3(1) E-Commerce Directive.
2247 Steinrötter, B./Schauer, L., Europäische Plattformregulierung, 1st ed. 2023, § 2 para. 67.
2248 Holznagel, B., *CR* 2023, 321, 322.
2249 Rec. 9 Regulation (EU) 2022/2065.

Recital 38 of the DSA contains a relaxation of the country of origin principle for orders to take action against illegal content and to provide information.[2250] As the orders in question relate to specific illegal content or information, they do not, in principle, restrict the freedom of these providers to offer their services across borders.[2251]

3. (Due diligence) obligations and liability of providers of intermediary services, Art. 4–48 DSA

The centrepiece of the DSA is Chapter II (Art. 4–10 DSA), which provides for liability privileges for intermediary services and thus does not offer a paradigm shift compared to the E-Commerce Directive. Chapter III, on the other hand, sets out extensive obligations for providers of intermediary services (Art. 11–48 DSA), which are based on the tiered system of liability.[2252]

a) General liability ng concept, Art. 4–6 DSA

aa) Liability privileges as a cornerstone of platform regulation

In recent decades, liability privileges for intermediary services have been fundamental to the further development of digital business models.[2253] The liability provisions of the DSA correspond almost exactly to the liability concept provided for in Art. 12–15 of the E-Commerce Directive.

It should be noted that the European legislator has expressly clarified in recital 17 that the liability privileges only stipulate when the providers are not liable. On the other hand, they are not to be regarded as a negative arrangement, according to which the service providers would always be liable if Art. 4–8 DSA are not relevant. Rather, the substantive legal basis for liability is to be found in Union law (e.g. Art. 130 EUTMR) and in national provisions, even if the DSA applies. Art. 4–8 DSA therefore do not establish liability, but rather limit it; to a certain extent, they represent a "filter" for the liability of intermediaries.[2254]

The DSA has adopted the horizontal approach of the E-Commerce Directive. It therefore covers all types of unlawful content and all types of liability.[2255] The wording "any liability" makes it clear that the provisions laid down in Art. 4–8 DSA apply irrespective of the otherwise applicable legal matter from which the substantive basis for liability arises.[2256] The horizontal regulatory approach implies that the liability rules are independent of sector-specific provisions of Union or national law. With regard to Member State law, this already results from the primacy of European law. Articles 4–8 of the DSA are

2250 For more details, see Holznagel, B., *CR 2021*, 123 et seq.
2251 Rec. 38 Regulation (EU) 2022/2065.
2252 Dregelies, M., *MMR* 2022, 1033 (1035).
2253 Legner, S., *ZUM* 2024, 99 (100).
2254 Janal, R., *ZEuP* 2021 227, 236.
2255 Rec. 17 Regulation (EU) 2022/2065.
2256 Hofmann, F./Raue, B., DSA, 1st ed. 2023, preamble to Art. 4 et seq. para. 6.

to be regarded as *leges specialis* and therefore take precedence over other European law. The applicability of the liability privileges means that further liability cannot be established by national legislation and EU law, as this is the only way to create a legally secure liability system.[2257]

The liability privileges form the cornerstone of the balance between the effective prevention of the dissemination of illegal content, the communication needs of users and the economic interests of service providers.[2258]

bb) Subjective scope: Information society services

The subjective scope of Art. 4 et seq. DSA covers **information society services**. It is unclear whether the subjective scope only covers the service providers themselves or also their employees and bodies.[2259] Depending on this, the liability exclusions would either only intervene in favour of the service providers or also privilege the activities of the employees and bodies.[2260]

cc) Material scope : Information provided by users

The prerequisite for liability privileges is that the object of the service is information provided by users, i.e. third-party information.[2261] A distinction must be made between information provided by the service provider itself.

Under the E-Commerce Directive, case law and literature had created the concept of "making it one's own".[2262] According to this, information that did not originate from the intermediary service itself but was "appropriated" by it was also "own". Indications such as the verification of the content by the service provider served to differentiate between the two.[2263] This meant that content originating from a third party could still be attributed to the service provider. There were already doubts about this interpretation under the E-Commerce Directive[2264] and the ECJ had also never adopted the figure. The interpretation failed because it could not be found in the wording of the E-Commerce Directive.[2265] Subsequently, the ECJ ruled for the E-Commerce Directive that it follows from recital 42 of the Directive that the liability privileges should only apply where the activity is of a purely technical, automatic and passive nature.[2266] The criterion of "making available" should therefore also be abandoned for the DSA.[2267]

2257 Steinrötter, B./Conrad, A., Europäische Plattformregulierung, 1st ed. 2023, § 3 para. 31 et seq.

2258 Steinrötter, B./Conrad, A., Europäische Plattformregulierung, 1st ed. 2023, § 3 para. 13; Legner, S., *ZUM* 2024, 99 (100).

2259 Steinrötter, B./Conrad, A., Europäische Plattformregulierung, 1st ed. 2023, § 3 para. 58.

2260 Steinrötter, B./Conrad, A., Europäische Plattformregulierung, 1st ed. 2023, § 3 para. 57 et seq.

2261 Wording of Art. 4 - 6 Regulation (EU) 2022/2065.

2262 See only German Federal Court of Justice (BGH); 14. Jan. 2020, cases VI ZR 496/18 and VI ZR 495/18 = *GRUR* 2020, 435 para. 39; German Federal Court of Justice (BGH), 4. Apr. 2017, case VI ZR 123/16 = *GRUR* 2017, 844 para. 18; Paschke, M./Berlit, W./ Meyer, C./ Kröner, L./ Petersdorff-Campen, T., TMG, 4th ed. 2020, § 7 para. 5.

2263 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 4 para. 39.

2264 For example Hennemann, M., 'TMG § 7', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 32 et seq.; Spindler, G./Schmitz, P., TMG, 2nd ed. 2018, § 7 para 8.

2265 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 4 para. 40.

2266 CJEU, 22. Jun. 2021, case C-682/18, C-683/18, = *GRUR* 2021, 1054 para. 105 - Youtube.

2267 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 4 para. 40.

Only those providers who play a passive role in the service are covered by Art. 4–6 DSA.[2268] If the service provider assumes an active role by obtaining knowledge and control over the information, the liability privileges are not applicable.[2269] The demarcation is therefore the central criterion for determining whether the privileges apply to them. The case law of the European Court of Justice on the E-Commerce Directive can be used for concretisation. According to this, the service provider may only assume the role of an "intermediary".[2270] It must provide its service neutrally by means of purely technical and automatic processing of the data entered by its customers.[2271] The decisive question is when the service provider still acts neutrally and when it leaves this role. Art. 4–6 DSA provide different connecting factors for this. For example, Art. 4 DSA is linked to an omission on the part of the service provider. The legislator has thus chosen an objective element to distinguish the neutral role from the active role. In contrast, Art. 6 DSA differentiates in its application according to whether the service provider has knowledge of the unlawful activity or content. Here, the legislator has provided for a subjective element in order to distinguish the passive from the active role.[2272] This coexistence of subjective and objective elements is also made clear in recital 18 of the DSA, according to which an active role is associated with knowledge (subjective) or control (objective). Recital 18 of the DSA stipulates that the service provider crosses the boundary of neutral activity by assuming editorial responsibility for the content. The legislator is thus establishing the criterion developed by the ECJ that the service provider no longer assumes a neutral position if, for example, it supports users in the distribution of digital content and assumes editorial responsibility.[2273] The service provider is then no longer a mediator of third-party information, but transmissions it into its own.[2274]

Recital 20 DSA provides for a limit to neutrality. According to this, neutrality cannot be assumed if the service provider co-operates with the user in order to carry out unlawful activities. On the other hand, the application of the liability privileges is excluded if the main purpose of the service provider's activity is to facilitate unlawful activities.

dd) Obligations of the individual mediation services

Art. 4–6 DSA each address one of the intermediary services listed in Art.(g) DSA.

(6) Pure transit, Art. 4 DSA

Article 4(1) DSA initially covers service providers whose service consists purely of transmission. According to Art. 4(1), Art. 3(g)(i) DSA, this refers to services that transmit information provided by a user or provide access to a communications network. They can then invoke the liability privilege if (a)

2268 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 4 para. 10.
2269 Rec. 18 Regulation (EU) 2022/2065.
2270 CJEU, 12. Jul. 2011, case C-324/09= *GRUR* 2011, 1025 para. 112 - L'Oréal*;* CJEU, 23. Oct. 2010, case C-236/08, C-238/08= *GRUR* 2010, 445 para. 112 - Google and Google France.
2271 CJEU, 12. Jul. 2011, case C-324/09= *GRUR* 2011, 1025 para. 113 - L'Oréal.
2272 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 4 para. 70.
2273 CJEU, 11. Sep. 2014, case C-291/13= *ZUM-RD* 2015, 425 para. 46 - Papasavvas.
2274 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 4 para. 70.

they did not initiate the transmission, (b) they did not select the addressee of the transmitted information and (c) they did not select or modify the transmitted information. Consequently, even if they are aware of illegal content, they are not responsible.[2275] According to recital 21 DSA, a modification of the content should not be considered if the service provider makes purely technical changes.

This privilege does not affect the possibility of court or official orders in accordance with Art. 4(3) DSA.

(7) Caching, Art. 5 DSA

Art. 5 DSA is aimed at caching services; the liability privilege of Art. 5(1) DSA covers caching. The caching service providers may (a) not change the information and must (b) observe the conditions for access to information. This means that the service provider must maintain the terms of use for the content provided if the information is only accessible to a limited extent.[2276] Thirdly, the caching service is required to (c) comply with the rules for updating information that are widely recognised and used in the industry. This is because constant updates are necessary to ensure the identity of the information on the host server and the cache memory.[2277] In addition, the caching service (d) must not interfere with the authorised use of technologies for collecting data on the use of information. It follows that, if the mirrored server legitimately collects usage data using a technology that is widely recognised and used in the industry, the caching provider must not restrict this.[2278] Finally, the caching service must also (e) act expeditiously in removing or blocking information it has stored as soon as it obtains actual knowledge that the information has been removed from the network at the original source of the transmission or access to it has been blocked or a judicial or administrative authority has ordered its removal or blocking. It is irrelevant whether the service provider itself becomes aware of the content it has cached. Recital 20 must be observed in this context, which specifies when the limit of the neutral role of the caching service is exceeded, which is particularly the case if its main purpose is to facilitate unlawful activities. According to recital 20, the encrypted transmission of information is not sufficient. Parallel to Art. 4(3) and Art. 6(4) DSA, Art. 5(2) DSA contains an exception for injunctive relief and removal claims. [2279]

(8) Hosting, Art. 6 DSA

Host providers can invoke a liability privilege under the conditions of Art. 6 DSA. A privileged service is the storage of information provided by the user. The decisive criterion is the service provider's knowledge of the illegal activities or content. On the one hand, the service provider must not have positive knowledge of the illegality of the content or activity. This means that the service provider must not be informed that the content has been made available illegally.[2280] The service provider is not expected to carry out an in-depth legal review, so the notice must contain sufficient information to enable the

[2275] Spindler, G., *MMR* 2023, 73, 75.
[2276] Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 5 para. 33.
[2277] Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 5 para. 35.
[2278] Steinrötter, B./Conrad, A., Europäische Plattformregulierung, 1st ed. 2023, § 3 para. 124.
[2279] Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 5 para. 40.
[2280] Steinrötter, B./Conrad, A., Europäische Plattformregulierung, 1st ed. 2023, § 3 para. 130 et seq.

service provider to recognise the illegality.[2281] In practice, the service provider is usually made aware of this through a third-party notification,[2282] in particular through the notification and redress procedure prescribed in Art. 16 DSA. The background to this is that the service provider leaves its neutral role, which is a prerequisite for the privilege of liability, as soon as it becomes aware of it.[2283]

In the case of claims for damages, the liability privilege does not apply if the service provider is aware of facts or circumstances that clearly indicate unlawful activity or unlawful content.[2284] In addition to positive knowledge, the liability privilege does not apply here if the unlawfulness was easily recognisable.[2285] The second exception to the liability privilege concerns the "notice-and-take-down" procedure. If the service provider subsequently becomes aware of the illegal content or activities, it will only continue to be privileged if it acts swiftly to block access to the illegal content or remove it.[2286] The obligation to act swiftly is not subject to rigid deadlines,[2287] but is made dependent on the type of illegal content reported and the urgency of the measures.[2288] Art. 6(3) DSA contains a special provision to protect consumers. This covers e-commerce platforms that are designed to enable consumers to conclude distance contracts with companies.[2289] According to this provision, the service provider may not invoke the liability privilege even if an average consumer can assume that the information or the product or service that is the subject of the transaction is provided either by the online platform itself or by a user under its supervision.[2290]

ee) Good Samaritan privilege, Art. 7 DSA

An innovation compared to the previous provisions of Art. 12–14 E-Commerce Directive is Art. 7 DSA – this is the so-called "**Good** Samaritan **Privilege**". [2291]

The background to the regulation is that service providers only benefit from the liability privileges if they assume a **neutral role** in the provision of the service. As a result, service providers run the risk of losing their liability privileges through measures that would actually be desirable because they could prevent infringements.[2292] Art. 7 DSA is therefore intended to create legal certainty and prevent the continued existence of false incentives not to take action.[2293] With the introduction of the good samaritan

2281 CJEU, 22, Jun. 2021, case C-682/18 C-683/18= *GRUR* 2021, 1054 para. 116 - YouTube and Cyando.
2282 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 6 para. 41.
2283 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 5 para. 36
2284 Art. 6(1)(a) Regulation (EU) 2022/2065.
2285 CJEU, 22. Jun. 2021, case C-682/18 C-683/18= *GRUR* 2021, 1054 para. 113 - YouTube and Cyando.
2286 Art. 6(1)(a) Regulation (EU) 2022/2065.
2287 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 6 para. 62 et seq.
2288 Rec. 52 Regulation (EU) 2022/2065.
2289 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 6 para. 55.
2290 Art. 6(3) Regulation (EU) 2022/2065.
2291 Rec. 26 Regulation (EU) 2022/2065.
2292 Sesing-Wagenpfeil, A., *MMR* 2023, 655, 656.
2293 Rec. 26 Regulation (EU) 2022/2065.

privilege, the legislator hopes to promote preventive measures such as content filters and create positive incentives to enable the detection of illegal content.[2294]

If the service provider takes measures that fulfil the requirements of Art. 7 DSA, the measure and any resulting knowledge of the illegal content should not be to its detriment.[2295] On the one hand, Art. 7 DSA stipulates that there is no risk of disadvantage,[2296] if the service providers take voluntary measures based on their own initiative, which they carry out carefully and in good faith[2297]. Secondly, Art. 7 DSA also applies to measures taken to comply with legal requirements. The second option concerns, in particular, measures to comply with Union law, including the DSA itself and those resulting from national legislation.[2298]

As a legal consequence, Art. 7 DSA stipulates that mediation services are eligible for the liability exclusions despite the measures mentioned. This means that the measures listed in Art. 7 DSA are to be disregarded when assessing whether the service provider assumes a neutral role. However, this does not mean that the service provider can automatically invoke Art. 4–6 DSA.[2299] As a result, Art. 7 DSA clarifies what was already widely recognised in case law for voluntary measures.[2300] Art. 7 DSA has also been criticised to the effect that, in the case of voluntary measures, unlawful content continues to trigger knowledge and, in this respect, liability would be established in the same way as without the measure.[2301] Art. 7 DSA therefore gives the service provider "stones instead of bread".[2302]

b) No general obligation to monitor or actively investigate, Art. 8 DSA

Art. 8 DSA exempts service providers from a general monitoring and investigation obligation. The prohibition thus flanks the liability privileges.[2303] In two directions, the service provider may neither be required to monitor transmitted or stored information nor to actively research it.[2304] Specific monitoring obligations and orders from national authorities are excluded.[2305] Art. 8 DSA therefore only refers to general obligations to monitor or investigate.

c) Judicial and official orders, Art. 9–10 DSA

Each of the liability privileges provides that Member State judicial or administrative authorities may require the cessation or prevention of an infringement in accordance with national law, Art. 4(3), 5(3) and 6(4) DSA. The orders are dependent on national legal systems;[2306] they find their legal basis there

---

2294 Legner, S., *ZUM* 2024, 99 (100) - (101).
2295 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 7 para. 12.
2296 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 7 para. 13.
2297 Rec. 26 Regulation (EU) 2022/2065 provides more details.
2298 Sesing-Wagenpfeil, A., *MMR* 2023, 655, 657 et seq.
2299 Rec. 26 Regulation (EU) 2022/2065; Sesing-Wagenpfeil, A., *MMR* 2023, 655, 658.
2300 E.g. CJEU, 22. Jun. 2021, cases C-682/18 and C-683/18 = *MMR* 2021, 705 para. 109 - YouTube and Cynado.
2301 Holznagel, B., CR 2021, 123 marginal No. 29.
2302 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 7 para. 10.
2303 Müller-Terpitz, R./Köhler, H., DSA,1st ed. 2024, Art. 8 para. 11.
2304 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 8 para. 13.
2305 Rec. 30 Regulation (EU) 2022/2065.
2306 Rec. 31 Regulation (EU) 2022/2065.

and follow the principles established there.[2307] The purpose of Art. 9 and Art. 10 DSA is to set minimum conditions for such orders. However, they do not constitute a legal basis for their issuance.[2308]

aa) Orders to take action against illegal content, Art. 9 DSA

The content of Art. 9 DSA refers to sovereign orders to take action against illegal content issued to providers of intermediary services. According to Art. 9(1) DSA, service providers are obliged to comply with orders and to inform the issuing authority of the nature and timing of the order. Art. 9(2)(a) DSA sets out standardised and binding formal minimum requirements throughout the EU that must be met in order to establish a duty on the part of the service provider.[2309] Art. 9(2)(b) DSA stipulates that the territorial scope of the order must be limited to what is strictly necessary. Recital 36 DSA specifies the requirement to the effect that the necessary extent generally includes the territory of the Member State. The procedure for transmitting the order and information on its execution is governed by paragraphs 3–6 of Art. 9 DSA.[2310]

bb) Requests for information, Art. 10 DSA

At the same time, Art. 10 DSA sets out requirements for an information order: As is already the case under Art. 9(1) DSA, Art. 10(1) DSA imposes an obligation on the service provider to execute and inform about the execution. Art. 10(2) DSA also establishes minimum content requirements. Art. 10(2)(b) DSA limits the scope of the order to the effect that it only relates to information that is already available, so that the service provider is not obliged to investigate.[2311]

d) Due diligence and transparency obligations for brokerage services

The counterpart to the liability privileges in Chapter III are the due diligence and transparency obligations set out in Chapter III.[2312] The DSA is based on a tiered system of due diligence obligations.[2313] The aim is to ensure responsible and diligent behaviour[2314] of the intermediary services and thereby create a safe and transparent online environment.[2315] The following description of the due diligence and transparency obligations is therefore based on the tiered system mentioned above.

aa) Level 1: Regulations for providers of intermediary services, Art. 11–15 DSA

At the first regulatory level are the obligations that apply to all providers of intermediary services (Art. 3 (g) DSA).

2307 Gerdemann, S./Spindler, G., *GRUR* 2023, 3 (7).
2308 Rec. 31 Regulation (EU) 2022/2065.
2309 Müller-Terpitz, R./Köhler, H./ Nägele, T., DSA,1st ed. 2024, Art. 9 para. 11.
2310 More detailed Müller-Terpitz, R./Köhler, H./ Nägele, T., DSA,1st ed. 2024, Art. 9 para. 20 et seq.
2311 Müller-Terpitz, R./Köhler, H./ Nägele, T., DSA,1st ed. 2024, Art. 10 para. 9.
2312 Hofmann, F./Raue, B., DSA, 1st ed. 2023, preamble to Art. 11 et seq. para. 1.
2313 Hofmann, F./Raue, B., DSA, 1st ed. 2023, preamble to Art. 11 et seq. para. 2.
2314 Rec. 3 Regulation (EU) 2022/2065.
2315 Rec. 40 Regulation (EU) 2022/2065.

(9) Contact point for authorities and users and legal representatives, Art. 11–13 DSA

Art. 11–13 DSA deal with the obligation to set up contact points for authorities and users, as well as the appointment of legal representatives. The background to this is that the DSA is not only intended to have a repressive effect, but also to promote cooperation with the intermediary services.[2316] The intermediary services must provide a central contact point with which the authorities of the Member States, the Commission or the Executive Board can contact them, Art. 11 DSA. The standard thus creates the possibility of simple and efficient communication with the service providers,[2317] by naming them (1) and providing the information required for communication (2), (3). The obligation under Art. 13 DSA is extended for service providers who do not have an establishment in the Union but offer services in the Union. They must also appoint a legal representative in the Member State in which they operate. This is intended to ensure effective supervision and enforcement of the provisions of the DSA.[2318] The legal representative must be sufficiently authorised to do so (2) and, if necessary, be personally liable (3). In order to enable communication, the contact details must be reported to the Digital Services Coordinator (4).

Art. 12 DSA serves to ensure fast, direct and effective communication with users,[2319] in which they can easily reach the service provider.[2320] Recital 43 mentions telephone numbers, email addresses, electronic contact forms and chatbots as examples. In principle, service providers are free to choose between the means of communication. However, they must provide the user with a means of communication that is not exclusively based on automated tools (Art. 12(1) DSA). The information about the contact point must in turn be published (Art. 12(2) DSA).

(10) GTC, Art. 14 DSA

Art. 14 DSA contains a special regulation for the **general terms and conditions (GTC)** of intermediary services. This is **a transparency obligation.**

The background to the regulation is that intermediary services delete content on the basis of their own, often stricter, terms and conditions.[2321] Art. 14 DSA is thus an expression of three basic statements of the DSA: private autonomy, transparency and balancing of interests. A balance is struck between the private autonomy of service providers and the freedom of users to use the services and provide information.

2316 Kaesling, K., *ZUM* 2021, 177, 178.
2317 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 11 para. 2.
2318 Rec. 44 Regulation (EU) 2022/2065.
2319 Rec. 43 Regulation (EU) 2022/2065.
2320 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 12 para. 2.
2321 Raue, B./Heesen, H., *NJW* 2022, 3537, 3540 para. 22.

If the service provider restricts this freedom of users, it is subject to the transparency obligation of Art. 14 DSA.[2322] Content moderation by the service provider should be foreseeable and comprehensible for the user, Art. 3(t) DSA.[2323] This creates the possibility of being able to judge the legality of restrictions that the platform has disclosed to users ex ante *ex post*.[2324]

Intermediary services must provide information in clear and comprehensible language on the extent to which user content can be restricted (Art. 14(1) DSA). This includes information on the guidelines, procedures, measures and tools they use to moderate content, in particular whether and to what extent algorithms are used (Art. 14(1) DSA). The requirements for the GTC, clear and plain language and easily accessible public form (Art. 14 (1) DSA), correspond to the requirements of Art. 3(1) P2BR.

The DSA does not provide for any restrictions on the content of general terms and conditions so as not to excessively restrict entrepreneurial freedom.[2325] This means that services do not have to allow all content, only if it is lawful, because there is no legal requirement to the contrary.[2326] In order to take sufficient account of the protection of minors, Art. 14(3) DSA stipulates that an intermediary service that is primarily aimed at or predominantly used by minors must explain its conditions and any restrictions in such a way that minors can also understand them. If the service provider makes changes, the user must also be informed of this in accordance with Art. 14(2) DSA.

According to Art. 14(4) DSA, the intermediary service provider must take into account the rights and legitimate interests of all parties and the fundamental rights of users when applying and enforcing the restrictions. Recital 47 DSA also extends this obligation to the design of the GTC.

It is unclear whether the DSA thereby establishes content control. If so, this would extend to the content in addition to the control and enforcement.[2327] The background to this could be that the design should not be left solely to the regulatory competence of the networks.[2328]

Another interpretation would be that this is merely an exercise control.[2329] In this case, Art. 14(4) DSA would only serve to enforce the content of the clause and would be limited to controlling the exercise.[2330]

Recital 45 DSA speaks in favour of an interpretation as content control. This includes the "content" of the GTC in the review. The purpose of Art. 14(1) DSA would also be rendered meaningless if the providers were to provide GTCs which they cannot exercise due to Art. 14 Para. 4 DSA.[2331] Furthermore, such an interpretation would contribute to the appropriate balancing of the fundamental rights enshrined

---

2322 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 14 para. 1.
2323 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 14 para. 2.
2324 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 14 para. 3.
2325 Legner, S., *ZUM* 2024, 99 (104).
2326 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 14 para. 2; previously Spindler, G., *CR* 2019, 238 para. 23.
2327 See Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 14 para. 76; Legner, S., *ZUM* 2024, 99 (105).
2328 Raue, B., *NJW* 2022, 209, 211 para. 14.
2329 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 14 para. 23.
2330 Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 35.
2331 Legner, S., *ZUM* 2024, 99 (105); Raue, B./Heesen, H., *NJW* 2022, 3537, 3540.

in the Charter of Fundamental Rights as intended in Art. 1(1) DSA. Service providers draw the line between freedom of opinion and information and the protection of individual interests by restricting content in their general terms and conditions. [2332]

The second interpretation can be based on the wording of Art. 14(4) DSA: This merely refers to the balancing of interests in application and enforcement. The ratio of the standard is to stipulate a non-discriminatory and non-arbitrary exercise of the GTC.[2333]

In German law, a parallel could be drawn with the case law of the Federal Court of Justice on the general terms and conditions of large and powerful social networks. Their freedom of organisation is to be restricted by the fundamental rights of their users,[2334] so that the Federal Court of Justice is aiming for a similar objective with its case law. However, it does not yet follow from this that Art. 14(4) DSA is a content review. On the one hand, the BGH's requirement for an objective reason and comprehensibility is also taken into account by a mere exercise control. Secondly, the DSA is fully harmonised Union law, which is therefore subject to an interpretation independent of national case law. The starting point of the BGH's decision is also decisive. This is aimed at a much smaller group of addressees than the DSA regulation and cannot be transmissionred from the individual case of the social media platform with market power to the totality of all intermediary services.[2335] As a result, the parallel should be recognised, but cannot be used as an argument for an interpretation.

(11) Transparency reporting obligations, Art. 15 DSA

The second transparency provision that applies to all intermediary services is Art. 15 DSA. According to this provision, service providers must publish a transparency report once a year, Art. 15(1) DSA. As with Art. 14 DSA, the ratio of the standard is the transparency and accountability obligation of service providers with regard to content moderation.[2336] The transparency report is intended to inform the public and the authorities about the moderation carried out by the service providers.[2337] Art. 15 DSA of the DSM applies in principle to all intermediary services, but differentiates in some respects between the service providers with regard to the obligations laid down. An exception is made in particular for micro and small enterprises (Art. 15(2) DSA). The content of the transparency report is set out in (1) in a catalogue of minimum requirements.[2338] According to Art. 15(1) DSA, service providers must formally make clear, easily understandable reports on the content moderation they have carried out in the relevant period publicly available once a year in a machine-readable format and in an easily accessible manner. The formal requirements can be specified by implementing acts of the Commission, Art. 15(3) DSA.

2332 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 14 para. 75.
2333 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 14 para. 23.
2334 German Federal Court of Justice (BGH), 29. Jul. 2021 = NJW 2021, 3179 para. 54 et seq.
2335 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 14 para. 24.
2336 Rec. 49 Regulation (EU) 2022/2065.
2337 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 15 para. 3.
2338 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 15 para. 9.

bb) Level 2: Rules for hosting services, Art. 16–18 DSA

The norm addressees of Art. 16–18 DSA are only intermediary services that are to be categorised as hosting services due to the storage of information provided by the user, Art. 3(g)(iii) or Art. 6 DSA.[2339] These are at the second level of the tiered regulatory system.

The background to the more extensive due diligence and transparency obligations is that hosting services play a particularly important role in dealing with illegal online content.[2340] The service providers store the information transmitted by users on their behalf and enable others to access sometimes considerable amounts of data. As a result, there is a need for simple reporting and redress procedures.[2341]

(12) Reporting and redress procedures Art. 16 DSA

Pursuant to Art. 16(1) DSA, hosting services are obliged to set up a reporting and remediation procedure to enable users and third parties to report illegal content (definition in Art. 3 DSA). Only content that does not comply with Union law or the law of a Member State is covered. Content that merely violates the contractual terms of use of the service provider is not covered.[2342] The illegality of the content is assessed according to Member State law, as the DSA does not specify any requirements in this regard.[2343]

The obligation to set up a notification and redress procedure arises from the liability privilege of Art. 6 DSA.[2344] Art. 16(3) DSA stipulates that a notification that reaches the service provider in the course of the notification and redress procedure prescribed by Art. 16 DSA leads to the service provider gaining concrete knowledge. Conversely, this results in the obligation to take swift action (Art. 6(1)(b) DSA). Art. 16 DSA establishes a 'notice-and-take-down system'. The aim is to ensure that the *notice* is facilitated by users or third parties.[2345] The procedure relates exclusively to the individual information notified and does not extend to other information - even if the same - that has not been notified, and therefore does not establish 'a stay-down obligation'.[2346]

Art. 16 DSA does not regulate what the consequences of the absence or non-implementation of a notification and remedial action procedure are for the privilege of liability. It could be considered to deny the service provider the privilege in the event of systematic disregard. Dogmatically, the exclusion could be linked to the requirement of a neutral service or a fiction of knowledge.[2347]

2339 Gerdemann, S./Spindler, G., *GRUR* 2023, 3 (8).
2340 Rec. 50 Regulation (EU) 2022/2065.
2341 Rec. 50 Regulation (EU) 2022/2065.
2342 Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 19.
2343 Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 21.
2344 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 6 para. 6.
2345 Kalbhenn, J./Hemmert-Halswick, M., *ZUM* 2021, 184, 118.
2346 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 16 para. 34.
2347 Gerdemann, S./Spindler, G., *GRUR* 2023, 3 (9).

According to Art. 16(1) DSA, the procedure must be easily accessible and user-friendly and allow for "transmission by electronic means". Examples of such a procedure would be **flagging systems** and **reporting buttons** which, when selected, lead to a web form.[2348] The necessary content of the notification, which must be cumulative, also follows from Art. 16(2) DSA. In particular, the report must contain a duly substantiated explanation from the user as to why the content is considered illegal (Art. 16(3)(a) DSA). The aim is to ensure that the hosting provider can take action by providing the necessary information.[2349] This is a favourable provision for the service provider, as only a notification that complies with the requirements of Art. 16(3) DSA also has the effect of establishing knowledge and thus liability (Art. 6(1)(b) DSA, Art. 16(3) DSA).[2350] The procedure following notification by the user or third party is specified in Art. 16(4)–(6) DSA. The hosting provider must make a prompt decision in accordance with Art. 16(6) DSA. A rigid time limit for blocking is not specified, so that prompt is to be interpreted on a case-by-case basis. Consequently, the requirements may vary considerably depending on the specific facts and circumstances and the type of content in question.[2351] The notification and remedial procedure must be considered in conjunction with Art. 17 DSA and the regulation for providers of online platforms in Art. 20 DSA, as it sets out rules on the remedial decision following the notification.[2352]

(13) Justification, Art. 17 DSA

The consequence of a report is necessarily a remedial decision, according to which the content is either left on the platform or a measure is taken against the content. Art. 17 DSA is not a basis for a remedial decision,[2353] but serves to ensure transparency of the moderation decision on which the restriction is based.[2354] According to Art. 17(1) DSA, the user concerned must be informed of the measure taken and a clear and specific justification must be provided. An exhaustive catalogue of restrictions requiring justification is provided for, which includes, for example, the restriction of the display of certain information provided, i.e. in particular the removal or blocking of content.

Art. 17 DSA is broader than Art. 16 DSA and refers to measures that are directed either against illegal content or content that violates the GTC.[2355] The minimum requirements for the statement of reasons are specified in Art. 17(3) and (4) DSA. Art. 17(3) DSA sets out a comprehensive catalogue of content requirements. Art. 17(4) DSA stipulates that the statement of grounds must be clear, comprehensible and reasonably accurate and specific.

2348 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 16 para. 13.
2349 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 16 para. 16.
2350 Gerdemann, S./Spindler, G., *GRUR* 2023, 3 (9).
2351 Rec. 62 Regulation (EU) 2022/2065.
2352 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 16 para. 32.
2353 Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 26.
2354 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA,1st ed. 2024, Art. 17 para. 2.
2355 Wording of Art. 17(1) Regulation (EU) 2022/2065.

(14) Reporting of criminal offences, Art. 18 DSA

If the hosting provider becomes aware of information that gives rise to suspicion of a past, present or future criminal offence, it must report this to the law enforcement or judicial authorities of the competent Member States. The purpose of the standard is to use the hosting provider as a source of information.[2356] Art. 18 DSA stipulates that the offence must be one that poses a threat to the life or safety of one or more persons. The requirements for the offence are not specified in more detail. Recital 56 of the DSA provides guidance, but only refers to examples of offences under Directive 2011/36/EU on preventing and combating trafficking in human beings, Directive 2011/93/EU on combating the sexual abuse of children or Directive (EU) 2017/541 on combating terrorism.

cc) Level 3: Additional provisions for online platforms, Art. 19–28 DSA

On the third level, Art. 19–28 DSA are aimed at online platforms (Art. 3(i) DSA). This is a hosting service that stores and publicly disseminates information on behalf of a user, provided that this activity is not merely an insignificant and purely ancillary function of another service or an insignificant function of the main service which, for objective and technical reasons, cannot be used without that other service, and provided that the integration of the ancillary or insignificant function into the other service does not serve to circumvent the applicability of this Regulation, Art. 3(i) DSA. This includes, for example, social networks and online trading platforms.[2357]

Micro and small enterprises are exempt from the requirements of Art. 19–28 DSA in accordance with Recommendation 2003/361/EC (Art. 19 DSA). The de minimis clause defines a materiality threshold above which micro and small enterprises are covered and below which they are to be protected from burdens. According to Art. 2(2) and (3) of Recommendation 20003/361/EC, providers with fewer than 50 employees and an annual turnover or annual balance sheet of up to ten million euros are privileged.

(15) Internal complaints management system, Art. 20 DSA

Compared to the E-Commerce Directive, Art. 20 DSA has been newly included. It requires online platforms to set up an electronic, easily accessible and free complaints procedure. The legal background to this regulation is the risk of so-called **overblocking** of lawful content.[2358] The internal complaints procedure is intended to strengthen user rights by giving the uploading user the opportunity to respond.[2359] Here too, the DSA is limited to establishing procedural requirements and does not provide any information about the outcome.[2360]

The complaints procedure must be accessible electronically and free of charge for six months from the time the user (Art. 17 DSA) or the reporting person (Art. 16(5) DSA) becomes aware of it (Art. 20(1) and (2) DSA). The authorised user is given the opportunity to lodge a complaint against the omitted

---

2356 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA,1st ed. 2024, Art. 18 para. 9.
2357 Rec. 13 Regulation (EU) 2022/2065.
2358 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 20 para. 2 et seq.
2359 Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 49.
2360 Kalbhenn, J./Hemmert-Halswick, M., *ZUM* 2021, 184, 118.

content moderation and against the content moderation that has taken place. In both cases, a prior notification is required. The second option for action, the complaint against moderation that has taken place, only relates to one of the catalogue decisions in (1)(a)–(d).[2361]

According to Art. 20(3) DSA, the complaints procedure must be easily accessible and user-friendly and enable the submission of precise and well-founded complaints.[2362] The complaints procedure is easily accessible and user-friendly if it is intuitive and easily recognisable.[2363] In contrast to Art. 21 DSA, the complaints procedure takes place between the service provider and the complainant without the need for external bodies to be involved.[2364] Users, including the reporting persons or organisations, are authorised to submit complaints (Art. 20(1) DSA); this does not include external third parties.

The service provider has no obligation to investigate or provide information. This means that the service provider can decide within the framework of the complaints procedure on the basis of the file, i.e. according to the facts presented.[2365] It could be criticised that no hearing of the 'other party' is stipulated; the only standard of review is the complaint. [2366]

In order to ensure a fair procedure,[2367] complaints must be processed "promptly, without discrimination, carefully and free from arbitrariness". Again, there is no rigid time limit within which the provider must take action. Furthermore, Art. 20(6) DSA requires that a human being is involved in the decision-making process (so-called **human-in-the-loop principle**). [2368]

The platform operator must decide within the complaints procedure whether the omission or the measure taken was unfounded. In other words, the subject of the decision is whether action was justified (Var. 1) or whether an omission would have been necessary (Var. 2). Depending on the outcome of the decision, the measure taken or the omission must be cancelled immediately (Art. 20(4) DSA). Art. 20(4) DSA is merely a procedural implementation obligation and not an individual right of the user.[2369] Despite this, Art. 20(4) DSA represents a rare obligation to act on a case-by-case basis in the DSA system.[2370]

(16) Out-of-court dispute resolution, Art. 21 DSA

In addition to Art. 20 DSA, the users concerned, including the reporting persons or organisations, have the option of invoking a certified out-of-court dispute resolution procedure in accordance with Art. 21 DSA. The out-of-court dispute resolution procedure is intended to provide both an alternative to the

2361 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 20 para. 43 et seq.
2362 Parallel provision Art. 16(3) Regulation (EU) 2022/2065
2363 Holznagel, B., *CR* 2022, 594, 597.
2364 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 20 para. 20; Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 55.
2365 Holznagel, B., *CR* 2022, 594, 598; Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 57.
2366 Holznagel, B., *CR* 2022, 594, 598.
2367 Rec. 58 (EU) 2022/2065.
2368 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 20 para. 64.
2369 Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 59.
2370 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 20 para. 81.

internal complaints procedure and a remedy against the decisions made there.[2371] The alternative solution to the internal complaints procedure should be viewed critically, as it does not fit into the escalation system set out in Art. 16, Art. 20 and Art. 21 DSA. It could be considered that a prior attempt at internal dispute resolution would be appropriate.[2372]

The choice of dispute resolution centre is at the discretion of the user. The parties are also obliged to co-operate with the body in good faith (Art. 21(2) DSA), whereby the duty to co-operate does not apply if the dispute has already been settled (Art. 21 (2) DSA). The point of reference for the decision is again the substantive law. The out-of-court dispute resolution body makes a court-like decision, which as such is not legally binding (Art. 21(2) DSA). Authorisation of the dispute resolution body follows the requirements set out in Art. 21(3) DSA and is granted upon application to the Digital Services Coordinator.

The costs of the proceedings are regulated in Art. 21(5) DSA and are borne asymmetrically. The platform operator bears the costs of the proceedings as well as reasonable reimbursement of the user's expenses if the user initiating the proceedings prevails. On the other hand, the user does not bear any procedural costs or reimbursement of expenses if they are unsuccessful.[2373] An exception is only appropriate if the user has clearly acted in bad faith and the abuse has also been established (Art. 21(5) DSA).

Uploading users and reporting parties can force the platforms to settle a dispute even if the moderation decision is flawless, without the risk of having to bear the costs. This user-friendly regulation should be viewed critically in its current form: The idea behind the out-of-court dispute resolution procedure was to incentivise the platform operator to make the "right" decisions (the so-called **prize-tag argument**).[2374] The incentive effect is to be achieved by the fact that incorrect moderation can be "priced" by the affected users.[2375] As a result, the cost-bearing regulation actually achieves the opposite. It makes legally compliant moderation more expensive, which in turn makes the desired moderation decisions more difficult.[2376] Due to the eligibility of both the affected user and the reporter, the platform operator is also faced with the conflict of being forced to settle the dispute out of court by one of the parties entitled to file a complaint, depending on the "severity" of the moderation decision.[2377] In addition, the fact that the dispute resolution centre is called upon by the user also results in a design-related partiality (so-called '*built-in trias*'). There is a risk of forum shopping, whereby the user chooses the dispute resolution body that decides in favour of the applicant.[2378] Ultimately, it could be considered that the user is already sufficiently protected by the possibility of internal complaint management opened up in Art. 20 DSA

[2371] Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (116).
[2372] Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 63.
[2373] Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 69.
[2374] Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 21 para. 76 et seq.
[2375] Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 70.
[2376] Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 21 para. 70.
[2377] Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 70.
[2378] Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 21 para. 72 et seq.

and that further protection is therefore not appropriate.[2379] The result of the obligation to participate and the cost-bearing regulation is that the platform providers are restricted in their entrepreneurial freedom (Art. 16 CFR).[2380] The conflict could only be resolved by significantly restricting the scope of Art. 21 DSA.[2381]

(17) "Trusted flagger", Art. 22 DSA

According to Art. 22 DSA, platform operators must set up mechanisms and processes that make it possible to prioritise the processing of reports that originate from certain trusted *flaggers*. The requirements for 'trusted flaggers' and their authorisation are specified in Art. 22(2) DSA. This categorisation is intended to result in an accelerated reporting procedure for reports submitted via the reporting procedure under Art. 16 DSA.[2382] The difference between Art. 16(7) DSA and Art. 22(2) DSA is that general notifications must be responded to promptly, while 'trusted flagger' notifications must be responded to immediately.[2383] In this respect, only time is prioritised. The Commission currently has a total of nine ‚trusted flaggers' from five Member States on its list.[2384]

(18) Measures and protection against misuse, Art. 23 DSA

The regulatory purpose of Art. 23 DSA, as evidenced by its title, is to protect against misuse of the online platform. The provisions of Art. 23 DSA cover two constellations that are mirror images of each other: On the one hand, the frequent and manifestly unlawful provision of illegal content by users (1). On the other hand, the frequent submission of obviously unfounded reports or complaints (2). The consequence of the existence of one of the abuse alternatives should be that the provider temporarily suspends the provision of the services or their establishment. In each case, this is preceded by a warning to the user. This does not affect the possibility for service providers to stipulate stricter sanctions in their general terms and conditions.[2385] The regulatory concept of Art. 23 DSA ensures that platform operators must take action against frequent and obvious abuse in order to protect the rights and interests of all parties involved.[2386]

(19) Transparency obligations, Art. 24, 27 DSA

Art. 24 and 27 DSA set out further transparency obligations. The information to be disclosed goes beyond the obligations applicable to all providers under Art. 14 et seq. DSA that apply to all providers. As a result, according to Art. 24(1) DSA, the requirements for the transparency report applicable to the online platform are extended compared to the general Art. 15 DSA.

2379 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 21 para. 79.
2380 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 21 para. 66.
2381 On reform proposals Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 21 para. 84.
2382 Steinrötter, B./Berberich, M., Europäische Plattformregulierung, 1st ed. 2023, § 5 para. 74 et seq.
2383 Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (118).
2384 For the current status, see the Commission's list at https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa (last accessed on 1 November 2024).
2385 Rec. 64 Regulation (EU) 2022/2065.
2386 Rec. 63 Regulation (EU) 2022/2065.

(a) Transparency reporting obligation of online platform providers, Art. 24 DSA

According to Art. 24(1)(a) DSA, providers of online platforms must list the number of disputes submitted to the out-of-court dispute resolution bodies referred to in Art. 21 DSA, the results and the duration of the mediation. In addition, according to Art. 24 (1)(b) DSA, they must disclose the number of suspensions in accordance with Art. 23 DSA, i.e. their activities to remove and block information that is considered illegal content or violates their general terms and conditions. According to Art. 24(2) DSA, they are also required to publish the average number of monthly active users. Correspondingly, the **Digital Services Coordinator** at the place of establishment and the Commission can request the information specified in (2) at any time. Finally, platform operators are obliged under Art. 24(5) DSA to disclose to the Commission the reasons for restrictions on use following the provision of illegal content (Art. 17(1) DSA).

(b) Transparency of recommendation systems, Art. 27 DSA

Art. 27 DSA is only aimed at service providers that use **recommendation systems**. They must set out in their general terms and conditions the most important parameters used in their recommendation systems, as well as all options for users to change or influence these important parameters (Art. 27(1) DSA). The requirement is concretised by Art. 27(2) DSA, which sets out certain minimum standards that the information must meet.

(20) Design and organisation of the online interface, Art. 25 DSA (*Dark Patterns*)

Consumers frequently do not make rational decisions in an economic sense, but are often subject to cognitive *biases* when making judgements and decisions; they unconsciously fall back on mental rules of thumb (heuristics), which are also known as mental shortcuts.[2387] Such rationality deficits make people susceptible to targeted and subtle manipulation, such as the conclusion of unwanted contracts, particularly in digital environments.[2388] One example of such manipulation is the pop-up windows or notices "The offer is only reserved for 60 seconds at the stated price!" often found on online hotel booking websites, which are intended to put pressure on consumers to conclude a contract.[2389] The European legislator considers such influencing strategies to be an inadmissible exploitation of certain behavioural and decision-making weaknesses by online platforms and intends to protect consumers with Art. 25 DSA.[2390]

Art. 25(1) DSA stipulates that online platforms must not design, organise or operate their online interfaces in such a way that users are deceived, manipulated or otherwise significantly impaired or hindered in their ability to make free and informed decisions. Art. 25 DSA thus addresses the phenomenon of so-

---

2387 In detail on rationality deficits: Weinzierl, Q., Dark Patterns und die Innere Sphäre der Grundrechte, p. 13 et seqq.

2388 Dregelies, M., *MMR* 2023, 243 (243).

2389 Martini, M./Drews, C./Seeliger, P./Weinzierl, Q., *ZfDR* 2021, 47, 47.

2390 Rec. 67 Regulation (EU) 2022/2065; Steinrötter, B./Schwamberger, S., Europäische Plattformregulierung, 1st ed. 2023, § 10 para. 87; Weinzierl, Q., *NVwZ* 2020, 1087, 1088, also states the need for regulation from an economic and constitutional perspective.

called '**dark patterns**'.[2391] According to recital 67 of the DSA, this refers to practices that are intended to or actually do significantly distort or impair the ability of users to make an autonomous and informed choice or decision. Online platforms are therefore prohibited from using certain design patterns in their user interfaces.[2392] These are very diverse in their design.[2393] The practical relevance and prevalence of 'dark patterns' was confirmed by a study commissioned by the European Commission in 2022, according to which 97% of the 75 most popular websites and apps in the EU use 'dark patterns'.[2394] The **European Commission** has reprimanded an infringement by the online platform ‚X' for deceiving users about how to obtain a verified status (so-called 'blue tick'). This is achieved by ‚X' designing and operating its interface in a way that deceives the user, as the blue tick can be obtained for a fee and is not dependent on an internal verification mechanism.[2395]

According to the wording, the protected group of persons are users, i.e. natural or legal persons who use an intermediary service (Art. 3(b) DSA). Recital 2 of the DSA clarifies that this includes commercial users as well as consumers.

The offences covered include the **design**, **organisation** (preparatory acts) and **operation** (use) of an online interface that deceives, manipulates or otherwise impairs the user. Due to the broad wording, Art. 25 DSA basically covers all acts that are likely to impair or hinder the user.[2396]

An action is unauthorised if users are deceived, manipulated or otherwise significantly impaired or hindered in their ability to make free and informed decisions.

Deception within the meaning of Art. 25(1) DSA means the misrepresentation of false facts.[2397] This includes practices such as the secret expansion of the shopping basket ('sneak into basket'), the unrecognised subscription ('hidden subscription'), ‚'disguised buttons/advertisements 'disguised buttons/ads') and confusing questions ('trick questions').[2398]

Manipulation refers to designs that deliberately influence or push users in a certain direction.[2399] This is characterised by creating and then disappointing users' expectations. This includes emphasised options for action (so-called 'framing/false hierarchy'), 'hidden information' and distraction (so-called 'misdirection'). The transition between the offences of deception and manipulation is often fluid.[2400]

2391 Rec. 67 Regulation (EU) 2022/2065.
2392 Dregelies, M., *MMR* 2023, 243 (244).
2393 Collection of various dark patterns in Martini, M./Drews, C./Seeliger, P./Weinzierl, Q., *ZfDR* 2021, 47, 52.
2394 European Commission, Behavioural study on unfair commercial practices in the digital environment, p. 120.
2395 https://ec.europa.eu/commission/presscorner/detail/de/IP_24_3761 (last accessed on 1 November 2024).
2396 Dregelies, M., *MMR* 2023, 243 (245).
2397 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 25 para. 20; *Kaesling*, NJW 2024, 1609, 1611.
2398 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 25 para. 21 et seq.; see also the overview in Martini, M./Drews, C./Seeliger, P./Weinzierl, Q., *ZfDR* 2021, 47, 52.
2399 Dregelies, M., *MMR* 2023, 243 (245).
2400 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 25 para. 25 et seqq.; Kaesling, K., *NJW* 2023, 1609, 1611.

In addition, any action that **otherwise** significantly **impairs** or **hinders** users in their ability to make a free and informed decision is also included as a fallback option. Design practices covered would be, for example, the creation of insurmountable obstacles or ‘forced review‘, where certain services are only possible if the provider's data protection conditions are accepted.[2401]

The wording of the standard is therefore very broad and can be understood as a general clause. The decisive factor is that the user's ability to make a free and informed decision is significantly impaired or hindered by the design (success of the offence).[2402] The term "significantly" depends on the individual case and is formulated in an open-ended manner.[2403] Due to the limitation to measures that impair or hinder, positive control effects (so-called ‘nudging‘) are not covered by the ban.[2404]

In order to cope with the diversity of the phenomenon and its legal containment, the Commission is authorised under Art. 25(3) DSA to issue guidelines for a more detailed classification of practices.

The regulation of the DSA is limited by the fact that, according to Art. 25(2) DSA, the provisions of the UCPD and the GDPR take precedence - in this respect, numerous practices to be classified as *dark patterns* are already covered by Art. 6 UCPD and the provisions of the GDPR, in particular Art. 6(1) GDPR.[2405]

(21) Online advertising and recommendation system, Art. 26 DSA

A further transparency obligation for online platforms can be found in Art. 26 DSA. The background to the regulation is the growing importance of online platforms and the new ways in which advertising is distributed on the platform (e.g. ‘*targeted advertising*‘).[2406] Providers of online platforms should therefore be obliged to make online advertising more transparent.

With this provision, the DSA follows on from the obligation of the advertiser to label the advertisement as provided for in the UCPD (Art. 7(2) UCPD).[2407] This obligation also applies to the provider of online platforms according to Art. 26(1) DSA. They must clearly indicate that the information is advertising (Art. 26(1)(a) DSA). In doing so, they can make use of voluntary standards in accordance with Art. 44(1)(h) DSA. This enables the user to make the decision not to receive content in the interests of their general freedom of action, which is protected by fundamental rights.[2408]

In addition, the user is protected from being misled,[2409] in that the provider of the online platform must identify the natural or legal person in whose name the advertisement is displayed (Art. 26(1)(b) DSA).

2401 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 25 para. 29 et seqq.
2402 Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 25 para. 67 et seq.
2403 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA, 1st ed. 2024, Art. 25 para. 11.
2404 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA, 1st ed. 2024, Art. 25 para. 12.
2405 Müller-Terpitz, R./Köhler, H./Barudi, M., DSA, 1st ed. 2024, Art. 25 para. 4 et seq.
2406 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 26 para. 1.
2407 Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (119).
2408 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 26 para. 11.
2409 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 26 para. 11.

In addition, in the case of paid advertising, the natural or legal person who has paid for the advertising must also be recognisable (Art. 26(1)(c) DSA). Finally, the user must be provided with meaningful information about the parameters used to determine the users to whom the advertising is displayed (Art. 26(1)(d) DSA). This is intended to prevent the potential risk of personalised advertising.[2410]

Furthermore, Art. 26(2) DSA stipulates that the provider of online platforms must offer users a function with which they can label commercial communications. The labelling function makes such labelling easier, particularly for product-placing influencers. The online platform ensures that this labelling is highlighted and enables other users to clearly and unambiguously identify the commercial nature in real time (Art. 26(2) DSA).

Art. 26(3) DSA prohibits the display of advertising based on ‚profiling' if personal data within the meaning of Art. 9(1) GDPR is used as input data.[2411] According to the definition of Art. 4(4) GDPR referred to in Art. 26(23) DSA, ‚profiling' is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. This includes so-called 'targeted advertising'.[2412]

(22) Transparency of recommendation systems, Art. 27 DSA

Recommendation systems are there to ensure that content is presented to the user in a curated manner. This algorithmic curation of content is a central component[2413] of the activities of online platforms. Art. 27 DSA takes this into account and provides for transparency obligations in connection with recommendation systems.

Recommendation systems are fully or partially automated systems that are used to suggest or prioritise certain information to users of online platforms on an online interface or to determine in some way the relative order or emphasis of the information displayed.[2414] These are filter tools that provide the user with a selection of information determined according to specific criteria.[2415]

Providers of online platforms that use such recommendation systems are required to disclose to users the most important parameters used in the recommendation systems (Art. 27(1), (2) DSA). The information must be provided in the general terms and conditions and must be written in clear and understandable language (Art. 27(1) DSA). The content must explain to the user why certain information is being proposed. This includes information about the criteria that are most important for determining the user (Art. 27(2)(a) DSA). In addition, the relative importance of the parameters must also be explained

2410 Steinrötter, B./Hoch-Loy, V., Europäische Plattformregulierung, 1st ed. 2023, § 4 para. 47.
2411 Hofmann, F./Raue, B./Grisse, K., DSA, 1st ed. 2023, Art. 26 para. 59.
2412 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 26 para. 44.
2413 Rec. 71 Regulation (EU) 2022/2065.
2414 Art. 3(s) Regulation (EU) 2022/2065.
2415 Hofmann, F./Raue, B./Grisse, K., DSA, 1st ed. 2023, Art. 27 para. 14.

(Art. 27(2)(b) DSA). The obligation to provide information is limited to the most important parameters.[2416]

According to Art. 27(3) DSA, the provider of the online platform must provide a selection and modification function that is accessible at all times.

(23) Online protection of minors, Art. 28 DSA

Taking into account the increased need to protect minors, providers of platforms that are accessible to minors are obliged to take proportionate measures in addition to the general requirements. This is intended to create a high level of privacy, security and protection for minors.[2417]

The scope is restricted by Art. 28(3) DSA. According to this provision, providers are not obliged to collect data on the age of their users. This means that the scope of Art. 28 DSA only addresses providers that are aimed directly at minors or are predominantly used by minors.[2418] The increased requirements for online platforms aimed at minors are an argument against them collecting data on the age of their users on their own initiative, which in turn thwarts the purpose of the standard and is likely to weaken the effectiveness of the protection of minors.[2419]

Providers that fall within the scope must take suitable and proportionate measures to protect minors in accordance with Art. 28(1) DSA. The required measures are only specified to the effect that they should serve the privacy, safety and protection of minors. A large number of different measures can be derived from this.[2420]

Art. 28(2) DSA is related to the general provision of Art. 26(3) DSA: According to this provision, no advertising may be displayed on the basis of profiling using the user's personal data.

(24) Further consumer protection provisions, Art. 30–32 DSA

Articles 30 - 32 of the DSA contain supplementary consumer protection provisions that only apply to providers of online platforms and enable consumers to conclude distance contracts with companies. The standard is aimed at B2C marketplaces. C2C platforms, on the other hand, are not covered.

The background to the regulation is that the online platform plays an intermediary role between traders and consumers. The purpose of Art. 30 to 32 DSA is therefore to facilitate the enforcement of existing consumer rights.[2421]

On the one hand, service providers must take precautions to ensure the traceability of companies (***know-your-business rule***). This is intended to prevent so-called fake shops and those that make it difficult to

[2416] Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 27 para. 36.
[2417] Rec. 71 Regulation (EU) 2022/2065.
[2418] Rec. 71 Regulation (EU) 2022/2065.
[2419] Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (119).
[2420] Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 27 para. 28.
[2421] Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (120).

enforce consumer rights due to missing or incomplete information.[2422] Art. 30(1)(a)–(e) DSA obliges service providers to ensure that businesses can only use their platform if consumers have received the necessary information in advance.[2423] Art. 30 DSA is a duty of care. The service provider must ensure that the company is not authorised to use the platform if it does not provide the information or if it concludes to the best of its ability that the information is not reliable and complete. [2424]

Furthermore, the DSA obliges service providers to design their platforms in such a way that companies can fulfil their duty to provide information (Art. 31(1) DSA). In particular, it must be possible for companies to provide information on the identification of their product and product safety and conformity in accordance with Art. 31(2) (a) and (c) DSA). The service provider must in turn verify the provision of this information to the best of its ability (Art. 31(3) DSA).

Ultimately, service providers must help consumers to enforce their rights in relation to unlawful products and services or to exercise them at all (Art. 32 DSA). Service providers are therefore obliged to inform consumers if a product or service is unlawful and to inform them of possible legal remedies (Art. 32(1) DSA). If it is not possible for the consumer to make contact, the service provider must make the information publicly and easily accessible (Art. 32(2) DSA). The decisive factor here is also the service provider's knowledge of the illegality of the content, as only then does the obligation to inform the consumer arise (Art. 32(1) DSA). Knowledge can result from an own-initiative investigation or a report, among other things.[2425]

dd) Stage 4: Regulations for very large platforms and very large search engines

Large digital platforms are an integral part of the infrastructure of the digital economy. They offer important marketing and sales channels for companies. At the same time, they enable opinions to be exchanged easily in the digital space and user-generated content to be distributed.[2426]

The obligations imposed on intermediary services are related to their social impact.[2427] The DSA recognises that ‘very large online platforms‘ (VLOPs) and ‘very **large** online **search engines‘** (VLOSEs) pose social risks that go beyond those of small platforms. This also means that they are subject to higher due diligence requirements.[2428] The background to the societal risks is that VLOPs and VLOSEs have a major influence on the formation of public opinion and public discourse as well as online trade. The

2422 Dregelies, M., *VuR* 2023, 175 (178).
2423 Name, address, telephone number and e-mail address (a); identity document (b); data of the payment account (c), if available an extract from the commercial register of a comparable register (d) and a self-certification to act in accordance with the law (e) Regulation (EU) 2022/2065.
2424 Dregelies, M., *VuR* 2023, 175 (179).
2425 Müller-Terpitz, R./Köhler, H./Föhlisch, C., DSA, 1st ed. 2024, Art. 32 para. 7.
2426 *Müller*, MMR 2022, 1007, 1007.
2427 Hofmann, F./Raue, B./Kaesling, K., DSA, 1st ed. 2023, preamble to Art. 33 et seq. para. 5.
2428 Rec. 76 Regulation (EU) 2022/2065.

DSA therefore aims to identify and prevent or at least minimise the potential risks and social or economic damage through effective regulation and enforcement.[2429]

The central provisions of the fifth section of the DSA are the tightening of the catalogue of obligations for online platforms and, as the "centrepiece",[2430] regulatory instruments that deal with the identification, assessment and minimisation of systemic risks (Art. 34 to 37, 39 to 41, 45 and 48 DSA).

The regulatory system is based on the ‘enforced self-regulation‘ approach. This means that the obligations are initially carried out under the company's own obligation (Art. 34, 35 DSA), but are regularly audited externally (Art. 37 DSA) and, if necessary, are subsequently subject to official supervision.[2431]

(25) Scope, Art. 33 DSA

Art. 33 et seq. DSA apply to online platforms (Art. 3(i) DSA) and online search engines (Art. 3(j) DSA) which have an average monthly number of at least 45 million active users in the Union and which are designated as very large online platforms or very large online search engines pursuant to Art. 33(4).

The decisive criterion for categorisation as VLOP or VLOSE is the average number of active users and therefore a case-by-case assessment (Art. 33(4) DSA). The relevant threshold is at least 45 million active users in the Union (Art. 33(1) DSA). The background to this figure is that this number of users accounts for 10% of the population of the Union. The DSA sets this as the threshold for assuming a significant reach above this level.[2432] Due to the constantly growing population, the Commission is authorised to supplement the operational threshold on an ongoing basis by means of delegated acts (Art. 33(2) DSA). The basis for determining the threshold is primarily the number of users to be reported by the providers in accordance with Art. 24(2) DSA, Art. 33(4) DSA.

The number of users is based on the number of active users, which is not necessarily the same as the number of registered users.[2433] The term **active user** of an online platform or online search engine is legally defined in Art. 3(p), (q) DSA: According to this, an **active user of an online platform** is a person who uses a platform either to provide information or to consume content published by the platform. In contrast, an **active user of an online search engine** is a person who submits a search query and can view the indexed information displayed by the search engine via its online interface (Art. 3(g) DSA). Recital 77 DSA concretises the undefined legal term "activity" to the extent that it refers to active use. In any case, it is sufficient that the user interacts with the information by clicking, commenting, linking, sharing, purchasing or carrying out transactions on an online platform.[2434] On the other hand, the owners of the websites indexed in the search results are expressly not covered.[2435] According to Art. 33(3) DSA,

2429 Rec. 79 Regulation (EU) 2022/2065.
2430 Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (122).
2431 Hofmann, F./Raue, B./Kaesling, K., DSA, 1st ed. 2023, preamble Art. 33 et seq. para. 10.
2432 Rec. 76 Regulation (EU) 2022/2065.
2433 Rec. 77 Regulation (EU) 2022/2065.
2434 Rec. 77 Regulation (EU) 2022/2065.
2435 Rec. 77 Regulation (EU) 2022/2065.

the Commission is responsible for adopting delegated acts to determine the delimitation criteria and methods.

In contrast to the DMA, only the number of users, but not the gatekeeping function or the impact of the platform on the internal market, is to be used for categorisation. Despite the different connecting factors, most of the platforms covered by Art. 33 et seq. DSA will also fulfil the requirements of the DMA, meaning that regulation is comparable in this respect.[2436]

As of now, the regulations of Art. 33 et seq. DSA cover 17 platforms, including 'YouTube', 'Amazon Store','Facebook',' Instagram' and two very large online search engines: 'Bing' and 'Google Search'.[2437]

(26) Tightening of the catalogue of obligations applicable to online platforms

The provisions that the DSA provides for the third level of regulation will be further tightened for online platforms. Specifically, this concerns the requirements for recommendation systems (Art. 38 DSA), online advertising (Art. 39, 46 DSA) and transparency reporting obligations (Art. 42 DSA).

According to Art. 38 DSA, VLOPs and VLOSEs are obliged to offer users a selectable option for the recommendation system that dispenses with profiling within the meaning of Art. 4 No. 4 GDPR. Art. 38 DSA thus goes beyond the transparency obligation provided for in Art. 27 DSA.

In addition to the transparency obligations for online advertising that apply to all platform providers and the limited ban on profiling under Art. 26 DSA, Art. 39(1) DSA also requires VLOPs and VLOSEs to set up a publicly accessible archive on their online interfaces. This archive should contain various information on the adverts placed.[2438] The necessary content of the archive is specified in Art. 39(2) DSA. It is clear from the wording at least that this is minimum information.[2439]

Amazon was appointed VLOP by resolution of 23 May 2023. As a result, Amazon was also obliged to make an advertising archive publicly accessible. Amazon took action against this obligation and complained about the disclosure of confidential information. The ECJ rejected this application in its ruling of 27 March 2024.[2440]

Furthermore, Art. 42 DSA expands the general transparency obligations of Art. 15 and 24 DSA to include additional reporting items. Firstly, Art. 42(1) DSA provides for an increased frequency of publication of the transparency reports. In addition, the VLOPs and VLOSEs must expand their transparency reports to include information on the staffing of content moderation as part of the reporting and complaints procedures in accordance with Articles 16, 20 and 22 DSA (Art. 42(2) DSA) and the average

2436 Hofmann, F./Raue, B./Kaesling, K., DSA, 1st ed. 2023, Preamble Art. 33 et seq. para. 6.
2437 Commission press release of 25 April 2023, available at: https://ec.europa.eu/commission/presscorner/detail/de/ip_23_2413 (last accessed on 1 November 2024).
2438 Steinrötter, B./Hoch-Loy, V., Europäische Plattformregulierung, 1st ed. 2023, § 4 para. 52.
2439 Steinrötter, B./Hoch-Loy, V., Europäische Plattformregulierung, 1st ed. 2023, § 4 para. 53.
2440 ECJ order of 27 Mar. 2024 - Case C-639/23 P (R), MMR-Aktuell 2024, 01422.

monthly number of users (Art. 42(3) DSA).[2441] The transparency obligation is supplemented by Art. 42(4) DSA, which is linked to the obligation under Art. 37 DSA for independent auditing.[2442] Providers are obliged to make available a report on the results of the risk assessment in accordance with Art. 34 DSA, the remedial measures taken in accordance with Art. 35(1) DSA, the audit report in accordance with Art. 37(4) DSA and the report on the implementation of the audit results in accordance with Art. 37(6) DSA.

(27) Risk assessment, Art. 34 DSA

Art. 34 DSA applies to the self-regulation of VLOPs and VLOSEs. They are obliged to identify, assess and analyse the systemic risks arising from the design, operation or use of the services and the associated systems, including algorithmic systems, or the use of their services (Art. 34(1) DSA).

The legislator is focussing on four risk categories. The risks arising from the dissemination of illegal content are to be recorded. The risk to VLOPs and VLOSEs due to the rapid and widespread dissemination of content is taken into account.[2443] The second risk category concerns the negative impact of the service on the exercise of the fundamental rights of the Charter, in particular freedom of expression and information and the right to respect for private life and data protection.[2444] It also covers risks that have a negative impact on democratic processes, social debate and electoral processes as well as public security.[2445] The last category covers risks to physical and mental health.[2446]

The risk assessment is carried out at least once a year (Art. 34(1) DSA). In terms of content, the catalogue of Art. 34 (1) DSA reflects the four risk categories described. The catalogue includes:

- Dissemination of illegal content (**a**),
- any actual or foreseeable adverse effects on the exercise of fundamental rights (**b),**
- actual or foreseeable adverse effects on social debate, electoral processes and public safety (**c)**,
- actual or foreseeable adverse consequences in relation to gender-based violence, the protection of public health and minors, and serious adverse consequences for the physical and mental well-being of a person **(d).**

In any event, it is sufficient that adverse effects are apparent; it is therefore not necessary, according to the wording, for there to be an actual unlawful impairment.[2447]

In particular, service providers must consider whether and how the factors listed in Art. 34(2) DSA influence the systemic risks. These factors include

- Design of the recommendation systems and other relevant algorithmic systems (**a)**,

2441 Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (122).
2442 Steinrötter, B./Hoch-Loy, V., Europäische Plattformregulierung, 1st ed. 2023, § 4 para. 38.
2443 Rec. 80 Regulation (EU) 2022/2065.
2444 Rec. 81 Regulation (EU) 2022/2065.
2445 Rec. 82 Regulation (EU) 2022/2065.
2446 Rec. 83 Regulation (EU) 2022/2065.
2447 Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (123).

- Systems for moderating content **(b)**,
- applicable general terms and conditions and their enforcement **(c),**
- Systems for the selection and display of advertising **(d)**,
- data-related practice of the provider **(e)**.

VLOPs and VLOSEs are obliged to retain risk assessment documents for at least three years in accordance with Art. 34(3) DSA.

(28) Risk minimisation, Art. 35 DSA

Art. 35 DSA responds to the systemic risks identified in accordance with Art. 34 DSA. The provider is obliged to take appropriate, proportionate and effective risk mitigation measures that are tailored to the systemic risks identified in accordance with Art. 34 DSA. Therefore, Art. 35 DSA is a further building block of enforceable self-regulation, as the providers themselves are primarily obliged to take measures to address the identified risks.[2448]

The limits of the measures lie in the fact that they must be appropriate, proportionate and effective. Therefore, VLOPs and VLOSEs must take all necessary measures, taking into account the economic capacity of service providers in the context of proportionality.[2449] The illegality of the content does not constitute a restriction. Rather, permitted behaviour and content may also be restricted in order to reduce the risks.[2450]

When taking measures, the service provider must take into account the fundamental rights of users in accordance with Art. 35(1) DSA. This applies in particular to freedom of expression.[2451] Art. 35 DSA thus indirectly refers to the categories of systemic risks, which include the negative impact on fundamental rights and on public security and electoral processes.[2452] The service provider must therefore maintain the balance between overblocking and underblocking.[2453]

Art. 35(1)(a)–(k) DSA contains a list of exemplary measures. Further details of the measures can be found in recitals 87 and 88 DSA. The measures to be taken under certain circumstances include

- Adaptation of the design, features or functionality of the services **(a),**
- Adaptation of the general terms and conditions and their enforcement **(b),**
- Adaptation of content moderation procedures [...] **(c),**
- Testing and adapting their algorithmic systems **(d),**
- Adapt their advertising systems and adopt targeted measures [...] **(e),**
- Strengthening internal processes, resources, auditing, documentation or supervision of their activities **(f),**

2448 Hofmann, F./Raue, B./Kaesling, K., DSA, 1st ed. 2023, Art. 35 para. 3.
2449 Rec. 86 Regulation (EU) 2022/2065.
2450 Hofmann, F./Raue, B./Kaesling, K., DSA, 1st ed. 2023, Art. 35 para. 15.
2451 Rec. 86 Regulation (EU) 2022/2065.
2452 Hofmann, F./Raue, B./Kaesling, K., DSA, 1st ed. 2023, Art. 35 para. 15.
2453 Müller-Terpitz, R./Köhler, H./Beyerbach, H., DSA, 1st ed. 2024, Art. 35 para. 7.

- Initiation or adaptation of cooperation with trusted whistleblowers pursuant to Art. 22 DSA and the implementation of decisions by out-of-court dispute resolution bodies pursuant to Art. 21 DSA **(g),**
- Starting or adapting cooperation with other providers of online platforms or online search engines on the basis of the codes of conduct or crisis protocols referred to in Article 45 and Article 48 **(h),**
- Awareness-raising measures and adaptation of online interfaces to provide users with more information **(i),**
- targeted measures to protect the rights of the child **(j),**
- Ensuring that an individual piece of information, whether generated or manipulated image, sound or video content, which bears a striking resemblance to an existing person, object, place or other entity or event and which falsely appears to a person to be genuine or truthful, is recognisable by a prominent marking when it is displayed on the online interface, and also providing a user-friendly function that allows users of the service to view such information **(point (k)).**

Art. 35(2) DSA clarifies another core component of the enforced self-regulation. This obliges the Digital Services Board (Art. 61 et seqq. DSA) to publish an annual report. This report is to be prepared in cooperation with the Commission and contain the most conspicuous recurring systemic risks and best practices for mitigation. The committee thus breaks down the best practices for minimising risk for VLOPs and VLOSEs[2454] and provides support for the self-regulation provided for in Art. 35(1) DSA.

Further assistance is provided by Art. 35(3) DSA, according to which the Commission, in cooperation with the coordinators, can issue guidelines for the application of Art. 35 DSA.

(29) Rapid response mechanism and protocols, Art. 36, 48 DSA

While Art. 34 and 35 DSA are aimed at the normal operation of the service provider, Art. 36 and 48 DSA are aimed at crisis situations in which the service provider must take additional measures. According to the DSA, a crisis occurs when exceptional circumstances arise that lead to a serious threat to public security or public health in the Union or in significant parts of the Union.[2455] For example, a crisis may be caused by an armed conflict, an act of terrorism, a natural disaster or a pandemic.[2456]

In these special cases, the Commission is authorised to issue decisions that require one or more VLOPs and VLOSEs to take special measures. Art. 36 DSA thus compensates for the fact that in "normal operation" the approach of self-government applies and the state must restrict the service providers' room for manoeuvre in individual cases due to its duty to protect.[2457]

Art. 36(1) DSA lists the measures that service providers may have to take:

2454 Spindler, *GRUR 2021*, 653, 659.
2455 Art. 36(2) of Regulation (EU) 2022/2065; Rec. 91 Regulation (EU) 2022/2065.
2456 Rec. 91 Regulation (EU) 2022/2065.
2457 Steinrötter, B./Denga, M., Europäische Plattformregulierung, 1st ed. 2023, § 6 para. 55.

- Assessment of whether, and if so, to what extent and how the operation and use of the services contribute or are likely to contribute significantly to a serious threat within the meaning of paragraph 2 (**a**);
- identify and apply targeted, effective and proportionate measures, such as measures referred to in Article 35(1) or Article 48(2), to prevent, eliminate or mitigate such contribution to the serious threat identified in accordance with point (a)[2458] (**point (b))**; and
- report to the Commission by a date specified in the Decision or at regular intervals on the assessments referred to in point (a), on the precise content, implementation and qualitative and quantitative impact of the targeted measures taken pursuant to point (b), and on any other issue related to those assessments or measures, as specified in the Decision (**point (c))**.

When determining and applying the measures, Art. 36(1) DSA stipulates that the principle of proportionality must also be observed here. The severity of the threat, the urgency of the measure and also the actual or potential impact on the rights and interests of all parties concerned must be taken into account.

The Commission decision must fulfil the requirements set out in Art. 36(3) DSA. The aim of the requirements is to ensure that the decision strikes a balance between effectiveness and proportionality.[2459] Therefore, the decision must contain measures that can be taken within a short period of time, but at the same time the crisis mechanism is only applied if and to the extent that this is absolutely necessary. The measures should be effective and proportionate at the same time.[2460] Article 36(3)(a) DSA therefore reiterates the principle of proportionality of the decision and its necessity. Pursuing the same restrictive purpose, Art. 36(3)(b) DSA stipulates that service providers must be given a reasonable period of time to take the measures. Finally, Art. 36(3)(c) DSA sets a time limit for the measures, according to which they may be imposed for a maximum of three months.

The further procedure for adopting a resolution is specified in Art. 36(4) DSA. According to this, the Commission must notify the providers of the decision once it has been adopted (a), publish it (b), inform the body, invite it to comment on it and keep it informed (c).

The VLOPs and VLOSEs are granted the right to choose the specific measures in Art. 36(5) DSA, despite the honourable restriction of the scope for decision-making in crisis situations. Pursuing a similar objective, the Commission can enter into a dialogue with the service provider on the effectiveness and proportionality of the measure in accordance with Art. 36(6) DSA.

To ensure the effectiveness of the decision, the Commission has the right to monitor the service provider in accordance with Art. 36(7) DSA. It must report its findings to the committee on a monthly basis. If the Commission is of the opinion that the measures taken are ineffective or disproportionate, it can

[2458] See Rec. 91 Regulation (EU) 2022/2065.
[2459] Steinrötter, B./Denga, M., Europäische Plattformregulierung, 1st ed. 2023, § 6 para. 60.
[2460] Rec. 91 Regulation (EU) 2022/2065.

request the service provider to review this by means of a decision after hearing the panel. This "second chance for the platform operator" in crisis situations must be critically assessed.[2461]

Art. 36(8) DSA stipulates a possibility to amend the decision in accordance with Art. 36(1) DSA and responds to the dynamics within crisis situations.[2462] The Commission can revoke the decision on the recommendation of the panel (a), but can also decide to extend it for a maximum of three months (b). According to (c), the measures can also be adapted in such a way that the experience gained in the application of the measures is taken into account.

If the Commission has adopted a decision pursuant to Art. 36(1), (7) or (8) DSA, it must fulfil an ongoing reporting obligation to the European Parliament and the Council, Art. 36(11) DSA.

In addition, Art. 48 DSA stipulates that the Commission may, on the recommendation of the panel, require VLOPs and VLOSEs to draw up voluntary crisis protocols. These are intended to provide for an intensified use of risk measures tailored to the acute situation.[2463]

(30) Independent audit, Art. 37 DSA

Art. 37 DSA requires service providers to undergo an independent audit at least once a year and at their own expense. The purpose of the regulation is to ensure that the obligations arising from the regulation and, where applicable, additional obligations from codes of conduct and crisis protocols are complied with.[2464] With Art. 37 DSA, the legislator intends to compensate for the scope for decision-making within the framework of self-regulation by monitoring service providers.[2465]

The scope of the audit is based on Art. 37(1) DSA and includes the obligations set out in Chapter II (a). In addition, obligations from codes of conduct (Art. 45 and 46 DSA) and the crisis protocols (Art. 48 DSA) are covered (b).

The audit procedure is set out in Art. 37(2) DSA. The auditor must base the audit method and audit standards on industry best practice and the applicable audit standards and codes.[2466] VLOPs and VLOSEs are expected to co-operate fully. They must provide the necessary support and co-operate with the auditors. To this end, they should grant the auditors access to relevant data and premises and respond to verbal or written enquiries.[2467]

In order to compensate for the auditor's extensive access to data, the auditor shall ensure an appropriate level of confidentiality and compliance with confidentiality obligations[2468]. On the other hand, the protection of the service provider should not adversely affect the performance of audits and other provisions

[2461] Steinrötter, B./Denga, M., Europäische Plattformregulierung, 1st ed. 2023, § 6 para. 68.
[2462] Müller-Terpitz, R./Köhler, H./Nägele, T./Dilbaz, S., DSA, 1st ed. 2024, Art. 36 para. 21.
[2463] Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (123).
[2464] Rec. 92 Regulation (EU) 2022/2065.
[2465] Steinrötter, B./Denga, M., Europäische Plattformregulierung, 1st ed. 2023, § 6 para. 71.
[2466] Rec. 92 Regulation (EU) 2022/2065.
[2467] Art. 37(2) Regulation (EU) 2022/2065.
[2468] Art. 37(2) Regulation (EU) 2022/2065.

of this Regulation, in particular the provisions on transparency, monitoring and enforcement.[2469] It is therefore particularly important to prevent the duty of consideration from having an impact on the scope of the audit.[2470]

Who is suitable as an auditor is defined in Art. 37(3) DSA. The audit must be carried out by an organisation that is independent and has no conflict of interest (a), has proven expertise in the field of risk management as well as technical skills and capacities (b) and can be shown to work with objectivity and in accordance with professional ethics (c). When a conflict of interest exists on the part of the audit organisation is specified in Art. 37(3)(a)(i)–(iii) DSA.

The result of the audit should be recorded in an audit report in order to enable a meaningful assessment of the audit.[2471] Its content is specified in Art. 37(4) DSA. It must contain the following information:

- Name, address and contact point of the provider and the period to which the audit relates (**a)**;
- Name and address of the audit organisation or audit organisations (**b**);
- Declaration of interests (**c)**;
- Description of the elements and methods tested (**d**);
- Description and summary of the most important findings (**e**);
- List of third parties that were consulted **(f**);
- Audit opinion as the conclusion of the audit (**g**);
- Recommendation in the event of a non-positive audit opinion (**h**).

The audit opinion provided for in Art. 37(4)(g) DSA should be emphasised. This indicates whether the service provider has complied with the audited obligations. It is divided into three categories: positive, positive with comments and negative.

According to Art. 37(6) DSA, the consequence of a non-negative audit report is that the service provider must take due account of the operational recommendations addressed to them and take the necessary measures to implement them. The service provider must in turn report on the implementation measures.[2472] However, the service provider does not have a mandatory obligation to implement the recommendations, rather the principle of 'comply-or-explain' applies[2473]: the measures can be followed or replaced by alternatives and a justification (Art. 37(6) DSA).

(31) Data access and control, Art. 40 DSA

Art. 40 DSA also serves to monitor VLOPs and VLOSEs. According to this, VLOPs and VLOSEs are obliged to grant access to data to various recipients.

2469 Art. 37(2) Regulation (EU) 2022/2065.
2470 Rec. 97 Regulation (EU) 2022/2065.
2471 Rec. 93 Regulation (EU) 2022/2065.
2472 Art. 37(6) Regulation (EU) 2022/2065.
2473 Gerdemann, S./Spindler, G., *GRUR* 2023, 115 (124).

Firstly, Art. 40(1)-(3) DSA regulates access to data by public sector bodies. According to Art. 40(1) DSA, the Digital Services Coordinator of the competent Member States or the Commission can assert the right of access. The rightful claimant must submit a "reasoned request", which only roughly defines the required procedure.[2474] The subject of the claim is data that is necessary for monitoring and assessing compliance with the Regulation.[2475] In more concrete terms, this includes data relating to algorithms and algorithms for training.[2476] The data access claim thus covers a core area of the activities of VLOPs and VLOSEs.[2477] In addition, the service provider has an obligation to provide explanations in accordance with Art. 40(3) DSA.

The right to data access entails a significant encroachment on the legal position of the service provider. Art. 40(2) DSA therefore stipulates that the use of data must be strictly earmarked.[2478] This should allow the rights and interests of the data subjects to be duly taken into account.[2479] In particular, the protection of personal data and confidential information and the protection of business secrets must be taken into account.[2480]

In addition, Art. 40(4) DSA grants a certain group of researchers a subjective legal right to data access.[2481] This entitlement is limited in personal and material terms. Only the authorised researchers specified in Art. 40(8) DSA are eligible. The right to data access should only be authorised in narrowly defined cases and for specific purposes.[2482] It is subject to strict purpose limitation. The data may only be used for the purpose of research that contributes to the detection, identification and understanding of systemic risks or that relates to the appropriateness, effectiveness and impact of risk mitigation measures.[2483]

The further regulation of the data access claim is described in more detail in Art. 40(4)–(12) DSA.

(32) Compliance department, Art. 41 DSA

According to Art. 41 DSA, the provider of VLOPs and VLOSEs is obliged to set up an independent **compliance department**. The term compliance refers to adherence to laws and regulations that affect companies.[2484] The compliance department forms the basis for compliance with the requirements of the DSA and is an important component of the concept of self-regulation.[2485]

2474 Müller-Terpitz, R./Köhler, H./Henn, S., DSA, 1st ed. 2024, Art. 40 para. 13.
2475 Art. 40(1) Regulation (EU) 2022/2065.
2476 Rec. 96 Regulation (EU) 2022/2065.
2477 Steinrötter, B./Denga, M., Europäische Plattformregulierung, 1st ed. 2023, § 6 para. 96.
2478 Steinrötter, B./Denga, M., Europäische Plattformregulierung, 1st ed. 2023, § 6 para. 98.
2479 Art. 40(2) Regulation (EU) 2022/2065.
2480 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 40 para. 20 et seq.
2481 Müller-Terpitz, R./Köhler, H./Holznagel, D., DSA, 1st ed. 2024, Art. 40 para. 26.
2482 Steinrötter, B./Denga, M., Europäische Plattformregulierung, 1st ed. 2023, § 6 para. 102.
2483 Art. 40(4) Regulation (EU) 2022/2065.
2484 Müller-Terpitz, R./Köhler, H./Linardatos, D., DSA, 1st ed. 2024, Art. 41 para. 2.
2485 Steinrötter, B./Denga, M., Europäische Plattformregulierung, 1st ed. 2023, § 6 para. 112.

The compliance department must have sufficient authority, powers and resources.[2486] In addition, direct access to the provider's management body must be provided. This also means that the management body bears overall responsibility.[2487] According to Art. 41(2) DSA, the management body must ensure that the compliance officer has the necessary qualifications to fulfil the tasks set out in (3). The specific requirements for the officer therefore depend on the company in question.[2488] Furthermore, the management body must appoint an independent head of the compliance department (Art. 41(2) DSA). The name and contact details of this person must be communicated to the Commission and the Digital Services Coordinator in accordance with Art. 42(4) DSA.

The duties of the compliance officers are defined in Art. 41(3) DSA. These include

- cooperation with the Digital Services Coordinator at the place of establishment and with the Commission for the purposes of the DSA (**a**),
- ensuring that all risks referred to in Art. 34 DSA are identified and properly reported and that appropriate, proportionate and effective risk mitigation measures are taken in accordance with Art. 35 DSA (**b**),
- the organisation and supervision of the activities of the provider of the systemically important platform in connection with the independent audit pursuant to Art. 37 DSA (**c**),
- informing and advising the management and employees of the provider of the systemically important platform about the relevant obligations arising from the DSA **(d**),
- monitoring the provider of the systemically important platform with regard to its obligations under the DSA (**e**) and
- where applicable, monitoring compliance with the commitments entered into by the provider of the systemically important platform under the codes of conduct pursuant to Art. 45, 46 DSA or the crisis protocols pursuant to Art. 48 DSA (**f**).

However, this catalogue is not to be understood as exhaustive, but merely as a supplement to the general obligations associated with a compliance mandate.[2489]

It follows from Art. 41(1) DSA that the compliance department should have an independent position. This requirement is further supported by the fact that, according to Art. 41(5) DSA, it is the responsibility of the management body to ensure independence.

[2486] Art. 40(1) Regulation (EU) 2022/2065.
[2487] Müller-Terpitz, R./Köhler, H./Linardatos, D., DSA, 1st ed. 2024, Art. 41 para. 7.
[2488] Müller-Terpitz, R./Köhler, H./Linardatos, D., DSA, 1st ed. 2024, Art. 41 para. 8.
[2489] Müller-Terpitz, R./Köhler, H./Linardatos, D., DSA, 1st ed. 2024, Art. 41 para. 17.

(33) Supervisory fees, Art. 43 DSA

The purpose of Art. 43 DSA is to ensure the financing of the additional regulatory burden associated with the DSA.[2490] For this reason, the Commission levies a supervisory fee. The supervisory fee is not at the discretion of the Commission, meaning that in principle every service provider is liable for the fee.[2491]

The specific calculation of the fees is only determined in principle by Art. 43(2), (5) DSA. The starting point is the estimate of the total amount of the annual costs incurred within the framework of the DSA, Art. 43(2) DSA. The estimate is made in advance and according to reasonable judgement.[2492] This total amount is then distributed in proportion to the size of the service and its average number of users.[2493] The exact amount of the supervisory fee depends on the services designated in accordance with Art. 33 DSA and is determined by an implementing act of the Commission for each provider, Art. 43(3) DSA. When calculating the fee, the Commission must apply the methodology to be determined by legal act in accordance with Art. 43(4) DSA. The Commission is therefore responsible for specifying the methodology, determining the limits and implementing the payment.[2494] In addition, the principles set out in Art. 43(5) DSA must be observed and the implementing acts must be adopted in accordance with the advisory procedure set out in Art. 88 DSA. In this way, the DSA endeavours to ensure the proportionality of supervisory fees.[2495]

In order to guarantee the purpose of Art. 43 DSA, Art. 43(6) DSA stipulates that the fees are external, earmarked revenue.

This does not affect the possibility of individual member states to demand a supervisory fee from providers if their main establishment is in their territory. The criteria for this can be found in recital 111 DSA, according to which the fee must be limited to what is necessary to cover costs and proportionate to the tasks.[2496]

4. Supervision and enforcement, Art. 49–63 DSA

The DSA is enforced in two parts at national and European level. The actors include the national authorities, the so-called **Digital Services Coordinators (DSC),** the **European Digital Services Board (EDPS)** and the **European Commission**.[2497]

2490 Rec. 101 Regulation (EU) 2022/2065.
2491 Müller-Terpitz, R./Köhler, H./Beyerbach, H./Seyer, T., DSA, 1st ed. 2024, Art. 43 para. 4.
2492 Rec. 101 Regulation (EU) 2022/2065.
2493 Rec. 101 Regulation (EU) 2022/2065.
2494 Hofmann, F./Raue, B./Kaesling, K., DSA, 1st ed. 2023, Art. 43 para. 21.
2495 Steinrötter, B./Denga, M., Europäische Plattformregulierung, 1st ed. 2023, § 6 para. 130.
2496 Hofmann, F./Raue, B./Kaesling, K., DSA, 1st ed. 2023, Art. 43 para. 12.
2497 Müller, K., *MMR* 2022, 1007, 1007.

a) Supervision and enforcement by the Member States, Art. 49–55 DSA

Articles 49 to 55 of the DSA regulate the part of the supervisory system that is the responsibility of the Member States. The DSA thus gives the Member States a primary government mandate. To this end, each Member State must appoint a **Digital Services Coordinator** by 17 February 2024 (Art. 49(2), (3) DSA). The coordinator is the main actor for enforcing the material obligations of the DSA.[2498]

The coordinator is responsible for coordinating the other national authorities in the Member State.[2499] It is also the point of contact for the Commission, the NEB and the DSC of other Member States.[2500] In order to fulfil its purpose as a central contact point, Art. 49(2) DSA stipulates that the DSC shall cooperate closely with the other national competent authorities, the Commission and the EDPS. If a Member State designates several competent authorities, the DSC is "first among equals" and hierarchically superior to the others.[2501] Nevertheless, the national authorities must work closely together to ensure a strong capacity to act at national level.[2502]

The coordinator must fulfil the requirements set out in Art. 50 DSA. Accordingly, the coordinator must act impartially, transparently and promptly in the fulfilment of its tasks. The Member States are obliged to provide the coordinator with sufficient financial and human resources, Art. 50(1) DSA.

In order to fulfil its duties, the DSC has the powers of investigation and enforcement standardised in Art. 51 DSA. The far-reaching instruments follow a graduated system with increasing intensity of intervention.[2503] The powers aim to be effective, dissuasive and proportionate[2504] and thus to be able to monitor compliance with the DSA and enforce the resulting obligations.[2505]

The investigative powers vis-à-vis providers of intermediary services that fall within its remit include

- the authorisation to request the transmission of information **(a),**
- the power to carry out inspections or to request a judicial authority in their Member State to order such inspections in any premises used by those providers or those persons for the purposes of their trade, business, craft or profession **(b),**
- the power to require all employees or representatives of providers to make statements on any information relating to the alleged infringement **(c).**

According to Art. 52(2) DSA, enforcement powers include the following:

- the authority to accept the commitments of these providers with regard to compliance with this Regulation and to declare these commitments binding **(a),**

2498 Hofmann, F./Raue, B./Rademacher, T., DSA, 1st ed. 2023, Art. 43 para. 7.
2499 Art. 49(2) Regulation (EU) 2022/2065.
2500 Rec. 110 Regulation (EU) 2022/2065.
2501 Steinrötter, B./Achleitner, R., Europäische Plattformregulierung, 1st ed. 2023, § 8 para. 15.
2502 Steinrötter, B./Achleitner, R., Europäische Plattformregulierung, 1st ed. 2023, § 8 para. 17.
2503 Müller-Terpitz, R./Köhler, H, DSA, 1st ed. 2024, Art. 52 para. 2.
2504 Art. 51(5) Regulation (EU) 2022/2065.
2505 Müller-Terpitz, R./Köhler, H, DSA, 1st ed. 2024, DSA, Art. 52 para. 2.

- the authority to order the cessation of infringements and, if necessary, impose remedial measures **(b),**
- the power to impose fines or to request a judicial authority in their Member State to do so, in accordance with Art. 52 DSA **(c),**
- the power to impose a penalty payment or to request a judicial authority in its Member State to do so, in accordance with Art. 52 DSA **(d),**
- the power to take interim measures to avoid the risk of serious harm or to request the competent national judicial authorities in their Member State to do so **(e).**

In addition, the DSC can utilise repressive enforcement powers under Art. 51(3) DSA. However, these are only to be used as a last resort if all other powers under Art. 51 DSA have been exhausted. This is a tiered regulatory system. The first step is to request the governing body to take all necessary measures, including the creation of an action plan (a) and the second step is to request the competent judicial authority to block the user's access to the affected service or, if this is not possible, to the online interface (b). In view of the intensity of the intervention, both on the part of the user and, where applicable, on the part of third parties, this is subject to strict conditions and is only possible in the event of serious damage and an offence against the life or safety of a person.[2506]

Companies also face sanctions with preventive (periodic penalty payments) and repressive (fines) effects. To this end, the member states issue provisions on sanctions, Art. 52 DSA. These must be effective, proportionate and dissuasive.[2507] The maximum amount of fines that can be imposed for non-compliance with an obligation laid down in this regulation is 6% of the worldwide annual turnover of the provider of intermediary services concerned in the previous financial year. Penalties may be imposed for providing incorrect, incomplete or misleading information, for failing to respond or to correct incorrect, incomplete or misleading information, or for failing to submit to an inspection, up to a maximum of 1% of the annual worldwide turnover of the provider of intermediary services or person concerned in the preceding financial year.[2508] The maximum amount of a periodic penalty payment may not exceed 5% of the average worldwide daily turnover or the average worldwide daily income of the provider concerned.[2509]

b) Compensation Art. 54 DSA

Systematically within the objective-legal monitoring and enforcement system, Art. 54 DSA regulates a subjective right of the individual. This follows from the fact that the user should always have a right to an effective and legal remedy before a court in accordance with national regulations.[2510]

2506 More detailed Müller-Terpitz, R./Köhler, H, DSA, 1st ed. 2024, Art. 52 para. 12.
2507 Art. 52(2) Regulation (EU) 2022/2065.
2508 Art. 52(3) Regulation (EU) 2022/2065.
2509 Art. 52(4) Regulation (EU) 2022/2065.
2510 Rec. 55 Regulation (EU) 2022/2065.

The DSA thus allows for individual legal enforcement, which users of intermediary services can use to claim compensation in such cases. The central claim standard for this is Art. 54 DSA. According to this, the user can claim damages if the service provider breaches user-related duties of care. Of particular relevance are the obligation to establish a reporting and redress procedure (Art. 16 DSA), the establishment of a complaints system (Art. 20 DSA) and the obligation for the provider to participate in out-of-court dispute resolution (Art. 21 DSA).

Art. 54 DSA is an imperfect liability standard. According to the wording, it must be applied in accordance with EU law and national law. In particular, this means that it is up to national law to specify the conditions of the claim and the legal consequences.[2511]

c) Coordinated investigations and coherence mechanisms, Art. 57 DSA

Due to the complex enforcement system at both Member State and European level, the DSA provides for close cooperation between the DSCs of the Member States, the Commission and the European body. The organisation of this cooperation is governed by Art. 57 DSA. The DSCs and the Commission are obliged to co-operate closely and provide mutual assistance, Art. 57(1) DSA. This obligation includes, in particular, the exchange of information between the DSC and the Commission as well as the obligation of the DSC to inform the Commission of the initiation of an investigation.[2512] The provision of information is concretised by granting the service provider the power to request other Digital Services Coordinators at the place of establishment to provide specific information about a particular provider of intermediary services that they hold or to exercise their investigatory powers in relation to specific information located in their Member State.[2513]

Finally, Art. 57(3) DSA contains an addition to the authorisation granted in Art. 57(2) DSA to request the provision of information. Among other things, the requested party must inform the DSC immediately and no later than two months after receipt. A refusal is only permitted in the cases regulated by Art. 57 (3)(a)–(c) DSA.

Across borders, Art. 58 DSA stipulates that the DSC of the destination should co-operate with that of the place of establishment of the service provider.

According to Art. 58(1) DSA, if the DSC at the place of destination considers that a service provider is infringing the provisions of the DSA and that this infringement is having a negative impact on users of the service in its Member State, it may request the DSC at the place of establishment to take investigatory and enforcement measures. In addition, in the event of a request from at least three DSCs at the place of destination, the political pressure on the DSC at the place of establishment can be increased by a request

2511 Müller-Terpitz, R./Köhler, H, DSA, 1st ed. 2024, Art. 54 para. 3; Legner, S., *ZUM* 2024, 99 (111).
2512 Art. 57(1) Regulation (EU) 2022/2065.
2513 Art. 57(2) Regulation (EU) 2022/2065.

from the European body, Art. 58(2) DSA.[2514] The content requirements for the request are set out in Art. 58(3) DSA.

If national authorities fail to fulfil their obligations under Art. 58 DSA and Art. 60(3) DSA, or do so inadequately, Art. 59 DSA constitutes an "escalation standard"[2515]. According to this, the body (Art. 61 DSA) can submit an alleged infringement to the Commission so that it can deal with it.[2516] The DSA thus provides for subsidiary supervision and enforcement by the Commission.[2517]

In order to make cross-border supervision more efficient, joint investigations can be initiated in accordance with Art. 60(1) DSA. This allows the DSC at the place of establishment to invite one or more other DSCs to conduct joint investigations. The cases in which joint investigations can be initiated are regulated in Art. 60 (1)(a) and (b) DSA. Other DSCs may request to participate in the investigation in accordance with Art. 60(2) DSA.

Communication between the competent bodies and authorities should take place via a reliable and secure information exchange system. Art. 85 DSA therefore requires the Commission to set up such a system.

d) European Digital Services Board, Art. 61–63 DSA

The European Digital Services Board is an independent advisory group of Digital Services Coordinators for the supervision of providers of intermediary services, Art. 61(1) DSA. The German-language abbreviation is "Gremium". The aim is to interlink the Member State and European levels. [2518]

The members of the panel are the coordinators for digital services, Art. 62(1) DSA. The Commission is not a voting member, but chairs the panel, Art. 62(2), (3) DSA. In addition, it provides administrative and analytical support for the activities of the body, Art. 62(4) DSA.

The purpose of the panel is to develop a common view of the Union and to promote cooperation between the competent authorities.[2519] The panel should therefore advise the Member State coordinators and the Commission in order to achieve the objectives set out in Art. 62(2)(a)–(c) DSA. This includes contributing to the uniform application of this Regulation and to effective cooperation **(a)** as well as coordinating and contributing to guidelines and analyses of the Commission, the Digital Services Coordinators and other competent authorities **(b)** and supporting the Digital Services Coordinators and the Commission in the supervision of very large online platforms **(c).**

In order to achieve these objectives, the committee must fulfil the tasks listed as examples in Art. 63(1)(a)–(e) DSA. Due to its role as an independent advisory group, the panel has no legal enforcement

[2514] Steinrötter, B./Achleitner, R., Europäische Plattformregulierung, 1st ed. 2023, § 8 para. 40.
[2515] Müller-Terpitz, R./Köhler, H, DSA, 1st ed. 2024, Art. 59 para. 3.
[2516] Art. 59(1) Regulation (EU) 2022/2065.
[2517] Steinrötter, B./Achleitner, R., Europäische Plattformregulierung, 1st ed. 2023, § 8 para. 43.
[2518] Hofmann, F./Raue, B., DSA, 1st ed. 2023, Art. 63 para. 10.
[2519] Rec. 131 of Regulation (EU) 2022/2065.

powers. The body's functions are limited to consultation and support.[2520] Art. 63 DSA can therefore be read as a kind of "general task clause"[2521], which authorises the panel to provide advice and support, but does not grant it any investigative or enforcement powers of its own.[2522]

The importance of the Committee derives from its '**copy or explain' function**, which is laid down in Art. 63(2) DSA. This is a formal obligation to take account of. Accordingly, Digital Services Coordinators and, where applicable, other competent authorities that do not follow the opinions, requests or recommendations addressed to them by the panel are required to give reasons for this. This is intended to ensure uniform application of the DSA.[2523] Measures taken by the panel are not legally binding.[2524] Instead, the legal consequences of a measure taken by the panel can be categorised into two stages. At the first stage, the DSCs and coordinators have a duty to familiarise themselves with and review the opinions, requests or recommendations. At the second stage, the measures must be justified in the event of a substantive deviation. This is therefore a formal but qualified duty of consideration.[2525] In addition to the general duty of care, the DSA has a number of more specific material duties of care. The legislator of the ordinance makes this clear by providing for consideration (Art. 60(4), Art. 91(7) DSA) or "taking into account" (Art. 36(10), Art. 58(4), Art. 59(3), Art. 66(4), Art. 75(1) DSA) of the panel's views.

e) Enforcement of obligations of providers of very large online platforms and very large online search engines

The DSA also recognises in its enforcement powers that VLOPs and VLOSEs are significant due to their scope and impact.[2526] For this reason, they are subject to stricter supervision. The Commission is the main body responsible for supervision. On the one hand, it has exclusive competence with regard to obligations specifically directed at VLOPs and VLOSEs (Art. 56(3), Art. 66 DSA). These include the obligation to assess (Art. 34 DSA) and minimise risks (Art. 35 DSA), to set up a crisis response mechanism (Art. 36 DSA), to carry out independent reviews (Art. 37 DSA) and to ensure the transparency of recommendation systems (Art. 38 DSA) and online advertising (Art. 39 DSA). On the other hand, it has shared responsibility for the obligations also directed at other service providers.[2527] Nevertheless, the Commission has a margin of discretion as to whether such shared responsibility is considered appropriate.[2528] The Commission's strong role is also strengthened by the fact that it is granted a prerogative position in enforcement vis-à-vis the national authorities.[2529]

2520 Steinrötter, B. /Keiler, S., Europäische Plattformregulierung, 1st ed. 2023, § 9 para. 25.
2521 Hoffman, F/Raue, B/Marsch, N, DSA, Art. 63 para. 1.
2522 Hoffman, F/Raue, B/Marsch, N, DSA, Art. 63 para. 1.
2523 Hoffman, F/Raue, B/Marsch, N, DSA, Art. 63 para. 18.
2524 Rec. 133 Regulation (EU) 2022/2065.
2525 Hoffman, F/Raue, B/Marsch, N, DSA, Art. 63 para. 22 et seq.
2526 Rec. 137 Regulation (EU) 2022/2065.
2527 Steinrötter, B./Achleitner, R., Europäische Plattformregulierung, 1st ed. 2023, § 8 para. 52; Hoffman, F/Raue, B/Krönke, C, Vorb. Art. 64 para. 2 et seqq.
2528 Rec. 125 and 139 Regulation (EU) 2022/2065.
2529 Steinrötter, B./Achleitner, R., Europäische Plattformregulierung, 1st ed. 2023, § 8 para. 54.

aa) Supervisory responsibility, Art. 66 DSA

Proceedings against VLOPs and VLOSEs are usually initiated in accordance with Art. 66 DSA. Such proceedings are initiated by the Commission if there is an actual suspicion against the service provider, Art. 66(1) DSA. The Commission is then obliged to inform the DCS and the panel.[2530] However, the initiation of proceedings is not a mandatory requirement for the Commission to exercise its investigative powers.[2531] In addition, the DCS have the option under Art. 65(2), (3) DSA to request the Commission to take action. If the obligation is not specifically addressed to the VLOPs and VLOSEs, the competent authorities of the Member State are only authorised to take action as long as the Commission has not yet initiated proceedings (Art. 66(2) DSA).

bb) Powers of the Commission

The powers of the Commission include

- Art. 67 to 69 DSA **Powers of investigation**: Powers to provide information (Art. 67 DSA), powers to question and take statements (Art. 68 DSA) and powers to carry out inspections (Art. 69 DSA)
- Art. 70 to 72 DSA **Powers to issue procedural orders**: Provisional measures (Art. 70 DSA), power to declare commitments binding (Art. 71 DSA) and the power to take supervisory measures (Art. 72 DSA)
- Art. 73–76, Art. 82(1) and (2) DSA **Powers to sanction and terminate proceedings**

The limits of their powers exist where they conflict with the rights of the persons subject to supervision. Taking this into account, Art. 79 DSA provides for a right to be heard and a right to inspect files. Art. 84 DSA draws a line where professional secrecy is threatened.

cc) Non-compliance and sanctions, Art. 73 ff DSA

Art. 73 et seqq. DSA regulates what VLOPs and VLOSEs are threatened with in the event of non-compliance. According to Art. 73(1) DSA, non-compliance means that the service provider does not fulfil the relevant provisions of this regulation (a), the interim measures ordered pursuant to Art. 70 DSA (b) or the binding commitments pursuant to Art. 71 DSA (c). In this context, the term "relevant provisions" must be interpreted narrowly, so that this only includes established infringements of provisions from Chapter III Section 5 (Art. 33 to 43 DSA) that fall within the exclusive area of responsibility of the Commission and established infringements of other provisions of a systemic nature that fall within the area of shared responsibility.[2532]

2530 Art. 66(2) Regulation (EU) 2022/2065.
2531 Art. 65(1) Regulation (EU) 2022/2065.
2532 Hoffman, F/Raue, B/Krönke, C/Petermair, D, DSA, Art. 35 para. 6.

The Commission is then authorised to issue a decision declaring non-compliance, Art. 73(1) DSA. The decision marks the end of the proceedings initiated under Art. 66 DSA.[2533]

Non-compliance can be penalised with fines and periodic penalty payments.[2534] The imposition and amount of the authorised fines is governed by Art. 74 DSA. Furthermore, Art. 76 DSA allows the imposition of periodic penalty payments to enforce compliance with obligations to act, tolerate or refrain from acting. In contrast, fines act as a repressive punishment for an infringement, while periodic penalty payments are intended to influence the future or current behaviour of the service provider.[2535] The setting of fines and periodic penalty payments must comply with the principle of proportionality and the prohibition of double jeopardy.[2536]

dd) Overview of sanctions[2537]

Infringement	Addressee	Regulation	(National) Fines
Failure to cooperate in the event of an official order to take action against illegal content	Mediation services	Art. 9 (1), (5) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Failure to cooperate in the event of an official order to provide information about a user	Mediation services	Art. 10 (1) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Failure to designate contact points for authorities	Mediation services	Art. 11 (1) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Failure to designate a contact point for users	Mediation services	Art. 12 (1) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Failure to publish/insufficient publication Contact points	Mediation services	Art. 11 (2), (3) Art. 12 (2) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Failure to appoint a legal representative	Intermediary services without establishment in the EU	Art. 13 (1), (2) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Omitted/inadequate/overdue notification of the legal representative	Intermediary services without establishment in the EU	Art. 13 (4) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Failure to inform about significant changes to the GTC	Mediation services	Art. 14 (2) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Not age-appropriate explanation of the GTC	Mediation services	Art. 14(3) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Omitted/insufficient/late transparency reports	Mediation services	Art. 15 (1), Art. 24 (1) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Missing/insufficient reporting procedure	Hosting service / online platform	Art. 16 (1), (2) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Omitted/inadequate/delayed notification of decision on notification and possible legal remedies	Hosting service / online platform	Art. 16 (5) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Inadequate moderation of illegal content	Hosting service / online platform	Art. 16 (6) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Omitted/inadequate/delayed justification of content moderation	Hosting service/online platform	Art. 17 (1), (2), (3), (4) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****

2533 Müller-Terpitz, R./Köhler, H/Henn, S., DSA, 1st ed. 2024, Art. 73 para. 22.

2534 For more details, see Steinrötter, B./Achleitner, R., Europäische Plattformregulierung, 1st ed. 2023, § 8 para. 84 et seq.

2535 Müller-Terpitz, R./Köhler, H/Henn, S., DSA, 1st ed. 2024, Art. 74 para. 3.

2536 Steinrötter, B./Achleitner, R., Europäische Plattformregulierung, 1st ed. 2023, § 8 para. 90.

2537 Source of the overview available at: https: //www.haufe.de/recht/weitere-rechtsgebiete/wirtschaftsrecht/leit faden-durchsetzung-des-digital-services-act-in-deutschland_210_628282.html (last accessed on 1.11.2024).

Lack of/inadequate access to an internal complaints management system	Online platforms	Art. 20 (1), (2), (3) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Failure to cancel/delayed cancellation of moderation after justified complaint	Online platform*	Art. 20 (4) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Failure to notify/insufficient/late notification to complainant	Online platform*	Art. 20 (5) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Decision was not made under the supervision of appropriately qualified personnel / exclusively automated	Online platform*	Art. 20 (6) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Lack of information on out-of-court dispute resolution under the DSA	Online platform*	Art. 21 (1) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Missing mechanism for trusted flagger	Online platform*	Art. 22 (1) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Failure to submit/insufficient/delayed submission of monthly active users in the EU at the request of the Digital Services Coordinator/EU Commission	Online platform / online search engine	Art. 24 (3) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Failure to submit/insufficient/delayed submission of decisions and justifications pursuant to Art. 17 (1) DSA for transparency database	Online platform*	Art. 24 (5) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Failure to cleanse the transmitted decisions and justification of personal data	Online platform*	Art. 24 (5) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Use of dark patterns	Online platform*	Art. 25 (1) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Omitted/inadequate advertising labelling	Online platform*	Art. 26 (1) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Lack of mechanism for users to label their content as advertising	Online platform*	Art. 26 (2) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Lack of recognisability of advertising labelling for other users	Online platform*	Art. 26 (2) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Display of personalised advertising using special categories of personal data (Art. 9 GDPR)	Online platform*	Art. 26 (3) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Lack of/insufficient transparency of the recommendation systems	Online platform*	Art. 27 (1), (2) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Lack of choice for users with multiple options for recommendation systems	Online platform*	Art. 27 (3) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Insufficient precautionary measures to protect minors	Online platform*	Art. 28 (1) DSA	Up to EUR 5,000,000
Personalised advertising if there is sufficient certainty that you are a minor	Online platform*	Art. 28 (2) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Lack of control of contractors prior to their utilisation	Distance selling platform*	Art. 30 (1) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Failure/insufficient/delayed request to correct mandatory information in the event of suspicion	Distance selling platform*	Art. 30 (3) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Failure to store/insufficient storage of mandatory data	Distance selling platform*	Art. 30 (5) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Disclosure of sensitive retailer information without good reason	Distance selling platform*	Art. 30 (6) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Failure to publish/insufficient publication of contact details, registration number if applicable and self-certification of the dealer	Distance selling platform*	Art. 30 (7) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**
Failure to design the platform so that traders can fulfil their information obligations (consumer protection, conformity, product safety)	Distance selling platform*	Art. 31 (1) DSA	Up to EUR 300,000 or up to 6% of annual worldwide **turnover****
Failure to provide information about unlawful product/service on platform	Distance selling platform*	Art. 32 (1) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**

Failure to publish information about unlawful product/service if consumer contact details are not known	Distance selling platform*	Art. 32 (2) DSA	Up to EUR 100,000 or up to 1 % of annual worldwide turnover**

5. Summary and implications for practice

In order to achieve its overarching goal of creating a safe, predictable and trustworthy online environment[2538], the DSA includes a comprehensive system of obligations and enforcement. The "heavy artillery" provided for by the DSA[2539] in the form of due diligence and transparency obligations as well as fines and periodic penalty payments apply to all providers of intermediary services. The scope of the DSA covers both the few globally operating VLOPs and VLOSEs as well as smaller providers of intermediary services.

The DSA always walks the fine line of balancing very different conflicting interests. For example, the DSA aims to effectively combat and prevent illegal content, thereby protecting the fundamental rights of platform users. On the other hand, there is the accusation that too much and too far-reaching content is deleted (so-called overblocking) and that there is too much interference in the entrepreneurial freedoms of the providers.

It is very welcome that the DSA creates a standardised legal landscape for such a cross-border field of activity as digital services. The DSA thus manages to protect the European area from fragmentation by national regulations and to prevent obstacles that hinder innovation.[2540] Service providers are faced with a total of 27 different regulatory systems if they want to operate across borders. Complying with these different and sometimes contradictory systems is cost-intensive and can only be managed by larger companies. The DSA will provide companies with a level playing field, making it easier for them to operate and grow across internal markets. The European Commission expects this to lead to a 2% increase in cross-border digital trade.[2541]

Suppliers of SMEs are exempt from the most cost-intensive obligations under Art. 29 DSA, which also promotes their growth. If an SME uses the online platform to sell its goods, it is subject to the terms and conditions of the major platforms and their internal handling of content. In this respect, the DSA provides SMEs with insight into the process of categorising their content, the advertising mechanisms and the moderation of their content through transparency obligations. The legislator hopes that this will make it easier for SMEs to grow and "take on the gatekeeper platforms".[2542]

2538 Rec. 9 Regulation (EU) 2022/2065.
2539 Wegmann, S./Kehl, J, *BB 2024*, 387, 387.
2540 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_de (last accessed on 1 November 2024).
2541 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act/europe-fit-digital-age-new-online-rules-businesses_de (last accessed on 1 November 2024).
2542 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act/europe-fit-digital-age-new-online-rules-businesses_de (last accessed on 1 November 2024).

On the other hand, companies are concerned that they will not meet the far-reaching due diligence and transparency obligations and will be confronted with the provisions on fines and damages.[2543] Nevertheless, the scope should not cause service providers to "panic".[2544] As a first step, service providers are required to check whether and, if so, under which category of the DSA they fall, which requires a careful examination. The second step is to determine which obligations apply to them. It should be noted that the application of the DSA may be broader than it appears at first glance and that even small companies are recommended to carry out an assessment of their risk profile.[2545] The advantage of the DSA is that it follows an asymmetrical regulatory system tailored to the size of the switching service. This is intended to ensure that service providers only face obligations that are proportionate. This could be countered by the fact that the comprehensive compliance obligations in particular are so high that they do not facilitate market access, but rather make it more difficult.[2546] It should also be taken into account that although the DSA is committed to the goal of creating legal clarity, there will still be questions of demarcation due to numerous undefined legal terms or vague obligations.[2547] In several places, the DSA provides that the Commission can adopt further legal acts to clarify the law[2548] or that the authorities can fill in the undefined legal terms in their inspections[2549], which emphasises that the DSA leaves room for further development. The DSA must therefore be recognised as creating a uniform regulatory system within the EU. However, it should be noted that the DSA has not created an exhaustive system that cannot be further specified. As a result, uncertainty will remain in some areas pending final clarification by the ECJ. Nevertheless, this is not a genuine problem of the DSA, but is inherent to the nature of a recent legal act. Furthermore, the legislator must be given credit for the fact that a field as dynamic as the data economy requires a flexible and adaptable regulatory system.[2550]

Another thrust of the DSA is to remedy the so-called *gatekeeper role* of the large platforms. This is to be achieved by increasing the transparency of the mechanisms for consumers. [2551] The powerful VLOPs and VLOSEs will also be subject to a series of comprehensive due diligence obligations, which will enable quick and predictable decisions through legal certainty. However, it remains to be seen whether the DSA will have a *Brussel effect* similar to the GDPR. This would be the case if regulatory law were to be modelled on the DSA. The resulting competition, the so-called '*race to the top'*, would be conducive to the aim of the DSA. On the other hand, it is also conceivable that service providers would try to

2543 Wegmann, S./Kehl, J, *BB 2024,* 387, 393.
2544 Schröder, C/Hardan, O, *BB 2023,* 579, 585.
2545 Wegmann, S./Kehl, J, *BB 2024*, 387, 393.
2546 Schröder, C/Hardan, O, *BB 2023*, 579, 585.
2547 Schmid, G/Greve, M, *MMR 2021,* 279, 282.
2548 E.g. Art. 15(3) DSA.
2549 Apel, S/Huber, C, *JuS 203*, 514, 518.
2550 Apel, S/Huber, C, *JuS 203,* 514, 518.
2551 Steinrötter, B./Hoch-Loy, V., Europäische Plattformregulierung, 1st ed. 2023, § 4 para. 1 et seq.

be subject to a less intensive regulatory system. The result would be a so-called race to the bottom, a "harmful deregulation spiral."[2552]

The system has been the subject of critique on account of its tendency to exaggerate matters. Whether this assumption that the obligations imposed are disproportionate to the risks is correct depends on how the risks are categorised. On the one hand, the far-reaching and strict liability framework could be welcomed in view of the threat of "civilisational decay".[2553] On the other hand, it should be recognised that in a liberal society, regulation, especially of freedom of expression, should always be treated as a last resort.[2554]

[2552] Steinrötter, B., Europäische Plattformregulierung, 1st ed. 2023, § 1 para. 19.
[2553] Geese, A, Why the DSA could save us from the rise of authoritarian regimes, https://verfassungsblog.de/dsa-authoritarianism/ (last accessed 1 November 2024).
[2554] Wegmann, S./Kehl, J, *BB 2024*, 387, 393.

VI. Digital Markets Act (DMA) - Regulation (EU) 2022/1925

Bibliography

Bechtold, R., Bosch, W., & Brinker, I. (eds.), EU-Kartellrecht, 4th ed., C.H. Beck 2023; Becker, B., "Privatrechtliche Durchsetzung des Digital Markets Act," *ZEuP* (2023), 403; Belloso, R., "The EU Digital Markets Act," 2022, accessible at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4109299; Brauneck, J., "Der Digital Markets Act (DMA) – das neue, bessere digitale EU-Wettbewerbsrecht?," *RDi* (2023), 27; Buchheim, J., Kraetzig, V., Mendelsohn, J., & Steinrötter, B. (eds.), Plattformen – Grundlagen und Neuordnung des Rechts digitaler Plattformen, Nomos 2023; Charbit, E., & Gachot, P. (eds.), Eleanor M. Fox: Antitrust Ambassador to the World – Liber Amicorum, 2021; Drewes, H., Meyer, L., & Moss, P., "Update: Europäische Plattformregulierung," *RDi* (2024), 310; European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679," Version 1.1, May 4, 2020, accessible at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf; Flechter, T., "DMA Switching Tools and Choice Screens," 2022, accessible at: https://cerre.eu/wpcontent/uploads/2022/11/DMA_SwitchingToolsandChoiceScreens.pdf; Galle, R., & Dressel, F., "Private Rechtsdurchsetzung des DMA," *EuZW* (2024), 107; Geradin, D., Bania, J., & Karanikioti, P., "The interplay between the Digital Markets Act and the General Data Protection Regulation," 2022, accessible at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4203907; Gersdorf, H., & Paal, B. (eds.), Beck'scher Online-Kommentar Informations- und Medienrecht, 44th ed., Status: 1 February 2023, C.H. Beck; Harta, J., "Marktmissbrauch und Digital Markets Act," *cepInput*, September 28, 2021, accessible at: https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepInput_Marktmissbrauch_und_DMA/cepInput_Marktmachtmissbrauch_und_DMA.pdf; Hebers, B., "Der Digital Markets Act ist verabschiedet – jetzt beginnt die Arbeit für alle Beteiligten," *BB* (2022), I; Higer, D., & Patt, C., "'Kampf gegen Windmühlen' – ist eine Abwendung der Gatekeeper-Benennung nach dem DMA tatsächlich überhaupt möglich?," *NZKart* (2024), 78; Kerber, W., "Datenrechtliche Aspekte des Digital Markets Act," *ZD* (2021), 544; Kersting, C., & Podszun, R., "Die 9. GWB-Novelle," C.H. Beck 2017; Kleine, M., Mienert, D., Moryn, K., & Timm, O., "Auf dem Prüfstand: Die Durchsetzung des DMA in der Digitalwirtschaft," *Newsdienst Compliance* (2024), 220008; Koenig, C., "Chapter 11: Introduction to the Digital Markets Act (DMA)," 2024, accessible at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4715147; Kraul, T. (ed.), Das neue Recht der Digitalen Dienste (DSA), Nomos 2023; Kraul, T., & Schmidt, H., "Plattformregulierung 2.0 – Digital Services Act und Digital Markets Act als Herausforderung für die Compliance-Organisation," *CCZ* (2023), 177; Küsters, S., "Stille Wasser sind tief – Zu den schwierigen Abgrenzungsfragen des Art. 3 Abs. 2 DMA," *BB* (2022), 2819; Möller-Klapperich, J., "Die Digitalisierung wirtschaftlich relevanter Sachverhalte und das (neue) Recht der Daten," *NJ* (2024), 193; Möller-Klapperich, J., & Rasquin, C., "Regulatorische Herausforderungen in KI-Wertschöpfungsketten," *NJ* (2023), 383; Monopolies Commission, Hauptgutachten – Wettbewerb 2022, Nomos 2022; Paal, B., & Kumkar, K., "Wettbewerbsschutz in der Digitalwirtschaft," *NJW* (2021), 809; Paal, B., & Pauly, D. A. (eds.), Datenschutz-Grundverordnung, 3rd ed., C.H. Beck 2021; Pfeiffer, L., & Helmke, J., "Die Digitalrechtsakte der EU (DGA, DSA, DMA, KI-VO-E und DA-E) – Teil I," *ZD-Aktuell* (2023), 01125; Podszun, R., Digital Markets Act – Handkommentar, 1st ed., Nomos 2023; Podszun, R., "Should Gatekeepers Be Allowed to Combine Data? Ideas for Art. 5(a) of the Draft Digital Markets Act," *GRUR Int.* (2022), 197; Podszun, R., Bongartz, P., & Kirk, A., "Digital Markets Act – Neue Regeln für Fairness in der Plattformökonomie," *NJW* (2022), 3249; Richter, A., & Gömann, M., "Private Enforcement des DMA – Ein Ausblick am Beispiel Amazons," *NZKart* (2023), 208; Riesenhuber, K., Europäische Methodenlehre, 4th ed., De Gruyter 2021; Säcker, F. J., Münchener Kommentar zum Wettbewerbsrecht, 4th

ed., C.H. Beck 2023; Savary, F., "Regulierung von Gatekeeper-Plattformen," *RDi* (2021), 117; Schmidt, J.P., & Hübener, F. (eds.), Das neue Recht der digitalen Märkte – Digital Markets Act, Nomos 2023; Steinrötter, B. (ed.), Europäische Plattformregulierung, Nomos 2023; Streinz, R., EUV/AEUV, 3rd ed., C.H. Beck 2018; Taeger, J., & Pohle, T. (eds.), Computerrechts-Handbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 39th ed., C.H. Beck 2024.

1. Introduction

The *Digital Markets Act* (hereinafter: DMA) was published in the Official Journal on 12 October 2022 and entered into force on 1 November 2022 in accordance with Art. 54(1) DMA. From 2 May 2023, the DMA will apply in all member states in accordance with Art. 54(2) DMA; it takes into account the growing importance of digital services, which are also increasingly more important for the functioning of the internal market within the Union.[2555]

a) Economic background of the DMA

Increasingly, market power can be observed to be centred on a few central platform services (so-called **gatekeepers**, Art. 1(2) DMA), which act as an economic interface between different groups of commercial and private users.[2556] The recitals to the DMA identify numerous reasons for this position of power, not least of which is the particular structure of the digital services market.[2557] Providers of centralised platform services benefit in particular from so-called **network effects**, whereby a distinction is made between direct and indirect network effects.[2558] Direct network effects arise when the utility value of a user increases the more members of the same user group the platform has.[2559] This applies in particular to users for commercial purposes due to the higher sales potential.[2560] Indirect network effects, on the other hand, occur in connection with multi-sided markets when the value and thus the growth of one demand group depends on the demand of another group.[2561] Platform providers benefit from these network effects in the form of rapid and exponential growth[2562]. At the same time, the addition of further users for platform services is hardly associated with marginal costs.[2563] In addition, end users generally only use one platform for a specific purpose, so there is no '**multi-homing**'.[2564] The largest platform usually wins.[2565] This leads to a high level of dependency on the respective platform service, especially

2555 Rec. 1 Regulation (EU) 2022/2065.
2556 Schmidt, J.P./Hübener, F./Mendelsohn, J./Budzinski, O., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 2 para. 2.
2557 Rec. 3 Regulation (EU) 2022/2065; Koenig, C., Chapter 11 Introduction to the Digital Markets Act (DMA), p. 6 et seq.
2558 Steinrötter, B./König, C., Europäische Plattformregulierung, 1st ed. 2023, § 11 para. 8.
2559 Schmidt, J.P./Hübener, F./Mendelsohn, J./Budzinski, O., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 2 para. 6; Kraul, T./Schmidt, H., *CCZ* 2023, 117 (183).
2560 Rec. 3 Regulation (EU) 2022/2065.
2561 MüKoEuWettbR/Bien, F., 4th ed. 2024, TFEU Art. 102, para. 258, 259; Schmidt, J.P./Hübener, F./Mendelsohn, J./Budzinski, O., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 2 para. 7.
2562 Rec. 2, 3, 13 Regulation (EU) 2022/2065.
2563 Rec. 2 Regulation (EU) 2022/2065; Savary, F., *RDi* 2021, 117 (118).
2564 Rec. 2 Regulation (EU) 2022/2065.
2565 Savary, F., *RDi* 2021, 117 (118).

for commercial users, as platform operators can control the access of other companies to important customer groups if they have the corresponding gatekeeper power.[2566] The dependence of commercial users on gatekeepers is flanked by the so-called **lock-in effect**[2567], which ensures that platforms bind their users to themselves so strongly that switching to alternative platforms would only be associated with higher switching costs and/or overcoming switching barriers - as a result, users regularly remain on the respective platform and do not even consider using competing platform services.[2568]

Last but not least, simplified access to large amounts of data for platform operators is becoming increasingly important in the age of AI.[2569] More users inevitably lead to more data, which in turn has a positive effect on the quality of the respective service and therefore attracts more users.[2570] This is also referred to as **data-driven network effects**.[2571] In addition, these data benefits can also spill over into other areas of the platform operator's activities, further consolidating its advantageous position.[2572]

The consequences of this development are manifold and their significance should not be underestimated: On the one hand, they have a detrimental effect on the choice available to users.[2573] On the other hand, innovation and fair competition are impaired, as market entry is hindered due to the structural advantages of existing platforms.[2574] This also harbours the risk of oligopoly formation.[2575] In addition to the enormously high investment costs, the poorer access to data is also of particular importance.[2576] In view of the special position of power of the providers of centralised platform services, there are also often divergent negotiating positions, which entail the risk of one-sidedly disadvantageous business conditions.[2577]

b) Objectives of the DMA

The DMA is intended to counteract the aforementioned risks and problems by creating guidelines for digital platform providers on how they may provide their services. According to Art. 1(1) DMA, the DMA is intended to contribute to improving the functioning and integration of the internal market by eliminating unequal competitive conditions for users and thus preventing fragmentation of the internal market.[2578] The aim is to harmonise legislation in order to ensure a contestable and fair digital market

---

2566 Steinrötter, B./König, C., Europäische Plattformregulierung, 1st ed. 2023, § 11 para. 7.
2567 Rec. 2 Regulation (EU) 2022/2065.
2568 Kraul, T./Schmidt, H., *CCZ* 2023, 117 (184); Savary, F., *RDi* 2021, 117 (118).
2569 Möller-Klapperich, J./Rasquin, C., *NJ* 2023, 383 (388).
2570 MüKoWettbR/Krämer, J., 4th ed. 2024, Ökonomische Grundlagen der digitalen Plattformregulierung, para. 56; Steinrötter, B./König, C., Europäische Plattformregulierung, 1st ed. 2023, § 11 para. 9.
2571 MüKoWettbR/Krämer, J., 4th ed. 2024, Ökonomische Grundlagen der digitalen Plattformregulierung, para. 56.
2572 Steinrötter, B./König, C., Europäische Plattformregulierung, 1st ed. 2023, § 11 para. 9.
2573 Rec. 2 Regulation (EU) 2022/2065.
2574 Rec. 4 Regulation (EU) 2022/2065.
2575 Rec. 2 Regulation (EU) 2022/2065.
2576 Rec. 3 Regulation (EU) 2022/2065.
2577 Rec. 4 Regulation (EU) 2022/2065.
2578 Rec. 7 Regulation (EU) 2022/2065; Koenig, C., Chapter 11 Introduction to the Digital Markets Act (DMA), p. 12 et seq.

throughout the Union.[2579] Platform providers that are (potentially) in competition with gatekeepers are to be strengthened in order to weaken the gatekeepers in their centralised position or at least create the impression that they are weakened.[2580] One of the aims of this is to ensure that gatekeepers do not independently abuse their market power vis-à-vis other companies and consumers.[2581] The DMA is therefore not only intended to protect competition on secondary markets, but also to attack and prevent the natural formation of monopolies in the digital economy.[2582] Nevertheless, the European legislator recognises that some gatekeepers are already so entrenched in their position that there is no longer any significant competition.[2583] In these cases, the measures of the DMA are intended to promote free competition on the downstream secondary markets and ensure fairness between the companies operating on these markets.[2584] Standardisation of regulations at European level can serve to exploit *economies of scale and scope* and reduce transaction costs.[2585]

c) Relationship to European and national competition law

The DMA is intended to take account of the special characteristics of digital markets and, in particular, competes with European and national competition regulations. Art. 1(6) DMA clarifies that the applicability of these provisions remains unaffected. However, the existing antitrust regulations have proven to be insufficient to achieve the concentration tendencies of digital groups that led to the enactment of the regulation.[2586] While previous regulatory instruments under competition law, namely the prohibition of abuse of a dominant market position (Art. 102 TFEU), only intervene *ex post*, the DMA is intended to have *an ex ante* effect for the addressee.[2587] A prior determination of unlawful behaviour is therefore no longer required under the DMA,[2588] rather, the DMA defines its addressees on the basis of formal criteria irrespective of their market power or cross-market significance.[2589] Although European competition law also applies in principle to the behaviour of gatekeepers, it is limited to specific incidents of market power, such as a dominant position on specific markets or certain anti-competitive behaviour.[2590] In addition, the aspect of fairness is more important in the context of the DMA than in the regulatory

2579 Rec. 8 et seq. VO (EU) 2022/2065.
2580 Steinrötter, B./König, C., Europäische Plattformregulierung, 1st ed. 2023, § 11 para. 20.
2581 Steinrötter, B./König, C., Europäische Plattformregulierung, 1st ed. 2023, § 11 para. 20.
2582 Schmidt, J.P./Hübener, F./Mendelsohn, J./Budzinski, O., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 2 para. 34.
2583 Rec. 32 Regulation (EU) 2022/2065.
2584 Steinrötter, B./König, C., Europäische Plattformregulierung, 1st ed. 2023, § 11 para. 22.
2585 Riesenhuber, K./Franck, J-U., Europäische Methodenlehre, 4th ed. 2021, § 5 para. 33.
2586 Rec. 5 Regulation (EU) 2022/2065.
2587 Schmidt, J.P./Hübener, F./Mendelsohn, J./Budzinski, O., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 2 para. 41, with further references.
2588 Schmidt, J.P./Hübener, F./Mendelsohn, J./Budzinski, O., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 2 para. 41, with further references.
2589 Art. 3(1), (2) DMA.
2590 Brauneck, J., *RDi* 2023, 27 (28).

purpose and in the provisions of European competition law.[2591] Although fair competition is also mentioned there, the aspect of fairness only plays a subordinate role, unlike in the DMA.[2592]

In future, official intervention on the basis of European competition law, in particular Art. 102 TFEU, should only be necessary in the case of actions by large digital groups if the DMA does not contain any corresponding provisions, if non-compliance with the requirements of the DMA can also be penalised as an infringement of the prohibition of abuse under Art. 102 TFEU and if it is linked to a significant market structure of the European internal market or threatens such a link.[2593] The abuse control therefore remains applicable in cases in which the gatekeeper fulfils the criteria of Art. 102 TFEU without its behaviour being related to a central platform service and/or constitutes a circumvention of the requirements of Art. 13 DMA.[2594]

The inconsistent regulatory provisions for digital services at national level have also led to a fragmentation of the internal market to date.[2595] Consequently, there was also a need for standardised regulations across Europe, which the DMA is intended to remedy.[2596]

d) Relationship to the Digital Services Act

In addition to the DMA, the DSA is also intended to contribute to fair and open digital markets. As a joint package on digital services, they form the first detailed set of rules for online platforms at EU level.[2597] The aim of the DSA is to create a safe, predictable and trustworthy online environment (Art. 1(1) DSA), focussing on the regulation of content on online platforms. However, the DMA ties in with the power structures typical of digital markets and is intended to counteract their fragmentation. Both pieces of legislation therefore target companies with positions of economic power, which can be traced back not least to the use of large amounts of data.[2598] There are also considerable differences between the regulations, which are manifested in the divergent objectives, but also in the different definitions, categories and requirements or, for example, the measurement of company sizes.[2599] In practice, however, there can sometimes be overlaps between the large technology companies, especially if companies are to be categorised as gatekeepers within the meaning of Art 2 DMA and also have to comply with the

---

2591 Bechtold, R./Bosch, W./Brinker, I., DMA, 4th ed. 2023 para. 12.
2592 Bechtold, R./Bosch, W./Brinker, I., DMA, 4th ed. 2023 para. 12.
2593 Monopolies Commission, main report Competition 2022, p. 233, 242.
2594 Monopolies Commission, main report Competition 2022, p. 241 et seq.
2595 Rec. 6 Regulation (EU) 2022/2065; at German level, Section 19a ARC should be mentioned here, which implements a special abuse control for large digital groups even if they do not hold a dominant market position but have a surprising cross-market significance for competition. Although the DMA also disregards national provisions, it is doubtful whether Section 19a ARC still applies at all due to the many parallels to the gatekeeper provision of the DMA in view of Art. 1(5) DMA; see in detail: Paal, B./Kumkar, K., *NJW* 2021 809 (815); Podzun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3250).
2596 Podzun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3250).
2597 https://www.consilium.europa.eu/de/policies/digital-services-package/ (last accessed on 1 November 2024).
2598 Möller-Klapperich, J., *NJ* 2024, 193 (193).
2599 Buchheim, J./Kraetzig, V./Mendelsohn, J./Steinrötter, B./Ruschemeier, H., Plattformen, 1st ed. 2024, p. 227 et seq.

provisions of the DSA as online service providers.[2600] With the provisions on ranking (Art. 2 no. 22 and Art. 6(5) DMA) and those on recommendation systems (Art. 3(s) and Art. 27 DSA), both regulations also cover the same subject matter.[2601] However, it is not clear from the respective legal texts how the two legal acts relate to each other in terms of substantive law.[2602] This is partly due to the fact that both regulations were proposed at the same time and were initially intended as a single regulation during the legislative process.[2603] In principle, it can be assumed that the two legal acts complement each other.[2604] However, how the two regulations relate to each other in the event of a conflict can ultimately only be decided on a case-by-case basis.[2605]

2. Material and territorial scope, Art. 1(2) DMA

The territorial scope of the DMA extends to the European Union. According to Art. 1(2) DMA, it applies to central platform services that provide or offer gatekeeper functions to business users or end users established or resident in the EU, regardless of whether they are based inside or outside the Union. Although the terms "providing" and "offering" are not defined in the DMA, the provision of necessary facilities and the willingness to provide services in the EU may be sufficient, following the example of the P2BR.[2606] From a material point of view, the DMA only applies to so-called *gatekeepers* in accordance with Art. 1(2) DMA. According to the legal definition in Art. 2 No. 1 DMA, these are companies that offer or provide centralised platform services for commercial users and end users and have been designated in accordance with Art. 3 DMA.

a) Central platform services, Art. 2 No. 2 DMA

Art. 2 No. 2 DMA lists an enumerative catalogue of services that are to be categorised as **central platform services**. These include:

- Online intermediary services (a);
- Online search engines (b);
- Online services of social networks (c);
- Video sharing platform services (d);
- number-independent interpersonal communications services (e);
- Operating systems (f);
- Web browser (g);
- virtual assistants (h);

2600 Buchheim, J./Kraetzig, V./Mendelsohn, J./Steinrötter, B./Ruschemeier, H., Plattformen, 1st ed. 2024, p. 227.
2601 Pfeiffer, L./Helmke, J., *ZD-Aktuell* 2023, 01125.
2602 Kraul, T./Nathanail, K., Das neue Recht der Plattformregulierung, 1st ed. 2023, § 2 para. 56.
2603 Buchheim, J./Kraetzig, V./Mendelsohn, J./Steinrötter, B./Ruschemeier, H., Plattformen, 1st ed. 2024, p. 227.
2604 Steinrötter, B./Schwamberger, S., Europäische Plattformregulierung, 1st ed. 2023, § 10 para. 4; see also: Kraul, T./Nathanail, K., Das neue Recht der Plattformregulierung, 1st ed. 2023, § 2 para. 56, whereby the latter cites Rec. 11 Regulation (EU) 2022/2065 as justification.
2605 https://www.nomos.de/digitalrecht-steinroetter/ (last accessed on 1 November 2024).
2606 Podzun, R./Käseberg, T./Gappa, S., DMA, 1st ed 2023, Art. 1 para. 9; MüKoEuWettbR/König, M., 4th ed. 2024, DMA Art. 1 para. 15.

- Cloud computing services (i) and
- online advertising services, including advertising networks, advertising exchanges and other advertising intermediation services provided by an undertaking providing one of the central platform services referred to in points (a) to (i) (point (j).

b) Appointment as gatekeeper, Art. 3 DMA

Art. 2 No. 1 DMA also requires that a company has been appointed as gatekeeper.

aa) Qualitative and quantitative thresholds, Art. 3(1), (2) DMA

Designation as a **gatekeeper** is made by the European Commission in accordance with Art. 3(1), (4) DMA, provided that the company

- has a significant impact on the internal market (a);
- provides a **central platform service** that serves commercial users as an important gateway to end users (b) and
- holds a stable and permanent position with regard to his activities or is likely to obtain such a position in the near future (c).[2607]

According to Art. 3(2) DMA, it is presumed that a company fulfils the respective requirements of Art. 3(1) DMA if it meets the quantitative thresholds specified in Art. 3(2) DMA.

According to Art. 3(2)(a) DMA, an undertaking is deemed to have a significant impact on the internal market if it has had an annual turnover in the Union of at least EUR 7.5 billion in each of the last three financial years or if its average market capitalisation or equivalent market value in the last financial year was at least EUR 75 billion and it provides the same core platform service in at least three Member States.

According to Art. 3(2)(b) DMA, it is presumed that the core platform service provided by an undertaking serves as an important gateway to end users for business users if it had at least 45 million monthly active end users established or resident in the Union and at least 10 000 annual active business users established in the Union in the previous financial year. According to Art. 2 No. 20 DMA, **an end user** is a natural or legal person who uses centralised platform services and does not act as a business user, i.e. does not use the centralised platform services for the provision of goods or services. The specific circumstances of the individual case must be taken into account; even fundamentally commercial actors can use platform services as end users in a particular situation.[2608]

The (probable) existence of an established and durable position is presumed under Art. 3(2)(b) DMA if these thresholds of end users and commercial users have been reached in each of the past three financial years.

[2607] Rec. 15 Regulation (EU) 2022/2065.
[2608] Rec. 14 Regulation (EU) 2022/2065.

bb) Designation procedure

If a company provides a central platform service, it must notify the Commission without delay in accordance with Art. 3(3) DMA in conjunction with Art. 21 DMA if it has reached all the thresholds specified in Art. 3(2) DMA. In addition, the notification must contain the information specified in Art. 3(2) DMA for each central platform service. The Commission must designate the company as gatekeeper within 45 days of receiving the complete information, Art. 3(4) DMA. According to Art. 3(5) DMA, the company also has the opportunity in this context to explain why it would exceptionally not fulfil the requirements set out in Art. 3(1) DMA, although it meets all the thresholds set out in Art. 3(2) DMA. However, if a company does not fulfil its notification obligation within two months of reaching the thresholds at the latest, the Commission can still designate the company as a gatekeeper on the basis of the information available to it in accordance with Art. 3(3) DMA.

If a company that provides central platform services does not meet the quantitative thresholds of Art. 3(2) DMA, but fulfils the requirements of Art. 3(1) DMA, the Commission still has the option of designating the company as a gatekeeper in accordance with Art. 3(8) DMA. To this end, it carries out a market investigation in accordance with Art. 17 DMA. When making the designation, the Commission must take various parameters into account in accordance with Art. 3(8) DMA, depending on the relevance for the respective company:

- Size of the company (a)
- Number of users (b)
- Network effects and data benefits (c)
- Economies of scale and scope (d)
- Lock-in effects (e)
- conglomerate-like corporate structures or the vertical integration of the company (f)
- other structural business or service characteristics (g)

Depending on the case, the EU Commission may include some or all of the aspects mentioned as well as foreseeable developments of the companies in its assessment (Art. 3(8) DMA). The Commission can also use this route to order compliance with certain behavioural obligations for companies that do not yet have an established market position, but where such a position is expected in the near future (Art. 3(1) DMA).

If the presumption criteria of Art. 3(2) DMA are met or if the presumption is based on the conditions of Art. 3(1) DMA, the Commission issues a designation decision pursuant to Art. 3(9) DMA. In this decision, the Commission names the relevant central platform services that act as an important gateway to end users for business users.

If a company argues that the presumption of conformity under Art. 3(2) DMA does not apply in its case, the EU Commission may reject these arguments within 45 working days if they are not sufficiently substantiated (Art. 3(5) DMA). However, if the Commission considers the arguments to be sufficiently

substantiated, it can initiate a market investigation within the deadline (Art. 3(5) DMA). This market investigation should be completed within five months (Art. 17(3) DMA) and aims to comprehensively examine the role of the company as gatekeeper before concluding with a published decision.

In accordance with Art. 3(10) DMA, the gatekeepers have six months from the date of appointment to implement the requirements of the DMA.

So far, the Commission has designated Apple (core platform services: App Store, Safari, iOS), Alphabet (core platform services: 'Google Search', 'Chrome', 'Android', 'YouTube', 'Google Maps', 'Google Play', 'Google Shopping', advertising services), 'Meta' (core platform services: 'WhatsApp', 'Facebook', 'Instagram', 'Meta Marketplace', advertising services), 'Amazon' (Central Platform Services: 'Amazon Marketplace', advertising services), 'Microsoft' (Central Platform Services: 'Windows', 'LinkedIn') and 'ByteDance' (Central Platform Service: 'Tiktok'). 'Apple' has also been a gatekeeper since 29 April 2024 with its central platform service 'iPadOS' and 'Booking' with its central platform service 'Booking.com' on 13 May 2024.[2609]

3. Obligations of the gatekeepers

a) Duty to cooperate, Art. 3(3) DMA

If the thresholds of Art. 3(2) DMA have been reached, companies providing central platform services are obliged under Art. 3(3) DMA to notify the European Commission independently and provide the relevant information. This must be done immediately, but at the latest within two months of reaching the thresholds. If a company already designated as a gatekeeper provides another central platform service that reaches the thresholds of Art. 3(2) DMA, it is subject to the same obligation.

b) Duties of conduct and omission, Art. 5–7 DMA

In particular, however, Articles 5, 6 and 7 DMA provide for numerous **obligations of behaviour and omission** for gatekeepers designated pursuant to Article 4(4) or (8) DMA with regard to the platform services specified in the designation decision pursuant to Article 3(9) DMA, which serve as an important gateway to end users.[2610] The obligations under Art. 5, 6 and 7 DMA are so-called **self-executing obligations**, i.e. they apply by operation of law without the need for a prior decision by any authority.[2611] According to Art. 13(3) DMA, these obligations must be fully and effectively implemented by the gatekeepers. Any behaviour that undermines effective compliance with the obligations under Art. 5, 6 and 7 DMA is prohibited under Art. 13(4) DMA. Art. 5 and 6 DMA differ in that Art. 6 DMA opens up further options for action by the Commission.

[2609] Commission press release of 6 September 2023, available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/de/ip_23_4328/IP_23_4328_DE.pdf (last accessed on 1 November 2024).

[2610] However, the obligations should also extend to digital products and services where gatekeepers use their function as an access gateway for themselves and which are often provided together with the central platform services or in support of them, see Rec. 31 Regulation (EU) 2022/2065.

[2611] Koenig, C., Chapter 11 Introduction to the Digital Markets Act (DMA), p. 20.

It regulates practices that undermine contestability in the digital sector and/or are considered unfair, as well as those that have a particularly negative direct impact on business users and end users.[2612]

The telos is to ensure **contestability** and **fairness** of the core platform services provided by gatekeepers by clearly and unambiguously defining obligations in relation to these services, taking into account the nature of these services, through harmonised rules for the entire internal market.[2613] This should be taken into account when interpreting the rules as an important guide to their purpose and meaning.[2614]

c) Obligations of gatekeepers in accordance with Art. 5 DMA

Firstly, the individual obligations of Art. 5 DMA will be discussed.

aa) Prohibition of data merging, Art. 5(2) DMA

Art. 5(2) DMA standardises prohibitions for gatekeepers with a reservation of permission with regard to the use and merging of data. In addition to ensuring fairness towards end users and the fundamental right to the protection of personal data in accordance with Art. 8 GDPR, the purpose of protection is also the fundamental separation of the respective data stock to ensure the contestability of digital markets.[2615]

bb) Prohibition of the processing of personal data for the purpose of operating online advertising services, Art. 5(2)(a) DMA

Art. 5(2)(a) DMA generally prohibits gatekeepers from processing **personal data** of end users who use third-party services that utilise the gatekeeper's central platform services for the purpose of online advertising. The data protection terms used in Art. 5(2) DMA are borrowed in full from the GDPR, as can be seen from the definitions in Art. 2 No. 24, 25, 26, 31 and 32 DMA. Thus, personal data - parallel to Art. 4 No. 1 GDPR - refers to all information relating to an identified or identifiable natural person. As in Art. 4 No. 2 GDPR, processing is to be understood as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, alignment or combination, restriction, erasure or destruction of data. Art. 5(2)(a) DMA therefore further restricts the processing purposes permitted under the GDPR.[2616] To date, gatekeepers have often collected personal data from end users for online advertising purposes when they use third-party websites and software applications.[2617] In addition, third parties provide gatekeepers with personal data of their end users themselves in order to be able to use certain services provided by the gatekeepers as part of their central platform services, e.g. advertising to user-defined target groups.[2618] The ban is intended

2612 Rec. 31 Regulation (EU) 2022/2065.
2613 Rec. 31 Regulation (EU) 2022/2065.
2614 Riesenhuber, K./Stotz, R., Europäische Methodenlehre, 4th ed. 2021, § 20 para. 17; Riesenhuber, K./Köndgen, J./Mörsdorf, O., Europäische Methodenlehre, 4th ed. 2021, § 6 para. 75-78.
2615 Podzun, R., DMA, 1st ed 2023, Art. 5(2) para. 10 et seq., 15.
2616 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 79.
2617 Rec. 36 Regulation (EU) 2022/2065.
2618 Rec. 36 Regulation (EU) 2022/2065.

to offset the advantages of gatekeepers in terms of data accumulation and thus reduce barriers to market entry.[2619]

cc) Prohibition of merging personal data, Art. 5(2)(b) DMA

Art. 5(2)(b) DMA generally prohibits gatekeepers from merging personal data from the respective central platform service with personal data from other central platform services or from other services provided by the gatekeeper or with personal data from third-party services. The **prohibition on merging data** applies in any case from the time the DMA takes effect. However, it is still unclear what impact this will have on existing databases fed from combined legacy databases.[2620] With regard to delimitability, it can be said that Art. 5(2)(b) DMA goes further than Art. 5(2)(a) DMA in that it covers not only the personal data of end users, but also that of commercial users.[2621] In addition, unlike the prohibition in Art. 5(2)(c) DMA, Art. 5(2)(b) DMA covers not only data from services controlled by the gatekeeper, but also data from third-party services without restriction.[2622]

dd) Prohibition of re-use of personal data, Art. 5(2)(c) DMA

Art. 5(2)(c) DMA generally prohibits gatekeepers from reusing personal data from the respective central platform service in other services provided separately by the gatekeeper, including other central platform services, and vice versa. It is questionable how the undefined legal term "reuse" is to be understood. In order to effectively protect the end customer and allow them to freely decide on their consent to the data processing and registration practices, the term *reuse* must be interpreted broadly in a systematically coherent manner, parallel to the term ‘data processing‘ under data protection law.[2623] In contrast to Art. 5(2)(b) DMA, the further use of data is included to the extent that it takes place without data merging.

ee) Prohibition of circumvention by notification, Art. 5(2)(d) DMA

Art. 5(2)(d) DMA generally prohibits gatekeepers from registering end users in other services of the gatekeeper in order to merge personal data. This requires both an objective component (registration of end users in other services) and a component of finality (purpose of merging personal data).[2624] It is unclear whether finality is to be understood subjectively in the sense of an intention to merge the data, or whether an objective interpretation is more appropriate. In favour of an objective understanding of the norm, the purpose of the norm with elements of data protection and competition law as well as the provision of Art. 8(1) DMA are put forward in addition to the historical references to abuse law case practice.[2625] According to this provision, the gatekeeper must ensure and prove compliance with the obligations under Art. 5, 6 and 7 DMA, from which it can be concluded that verifiable, i.e. objectively

---

2619 Rec. 36 Regulation (EU) 2022/2065.
2620 Podzun, R., DMA, 1st ed 2023, Art. 5(2) para. 18.
2621 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 87.
2622 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 87.
2623 Rec. 36 Regulation (EU) 2022/2065; MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 89.
2624 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 92.
2625 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 94.

demonstrable, measures are required to prove that a registration does not serve to merge personal data.[2626]

ff) Exceptions, Art. 5(2) DMA

Art. 5(2) DMA provides for two exceptions to the prohibitions on the use and merging of data.

On the one hand, the reservation of authorisation stipulated in Art. 5(2) DMA, insofar as the end user has been granted the specific choice and has effectively consented in accordance with Art. 4 No. 11 GDPR and Art. 7 GDPR in conjunction with Art. 2 No. 32 DMA. What is therefore required is a voluntary, informed and unambiguous expression of will in the specific case in the form of a declaration or other unambiguous affirmative act by which the data subject indicates that they consent to the processing of their personal data, Art. 4 No. 11 GDPR. The granting of a specific choice is likely to be identical to the characteristic of a declaration for the specific case (Art. 4 No. 11 GDPR).[2627] However, consent can be withdrawn at any time in accordance with Art. 7(3) GDPR. Due to the express reference of the DMA to the GDPR, its interpretation must be applied when applying the DMA.[2628] In addition to the case law of the European Court of Justice[2629], the guidelines of the European Data Protection Board in particular must be taken into account when interpreting the GDPR.[2630] Consent must also be interpreted in the light of Art. 25 DPA, i.e. the user must not be deceived, manipulated or otherwise significantly impaired or hindered in his ability to make free decisions by any design of the online interfaces on the part of their providers (so-called prohibition of 'dark patterns').[2631] In addition, Art. 5(2) DMA must be observed as a restriction, according to which the gatekeeper may not repeat its request for consent for the same processing purpose more than once within one year once the end user has refused or withdrawn consent.[2632] This is intended to prevent the end user from being bothered with continuous requests for consent (so-called '**nagging prohibition**').[2633] Art. 5(2) DMA in conjunction with Art. 7(1) GDPR stipulates that the gatekeeper must prove the existence of consent.

On the other hand, contrary to the aforementioned prohibitions, processing and merging is also permitted without consent if the gatekeeper can invoke the lawfulness of the processing pursuant to Art. 6(1)(c),

---

2626 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 94.

2627 Podzun, R., DMA, 1st ed 2023, Art. 5(2) para. 24.

2628 Podzun, R., DMA, 1st ed 2023, Art. 5(2) para. 21; Geradin, D./Bania, J./Karanikioti. P., The interplay between the Digital Markets Act and the General Data Protection Regulation, p. 7 et seq.

2629 See only *ECJ*, 11 Nov. 2020 - C-61/19, ZD 2021, 89, para. 35 et seq. - Orange Romania; *ECJ*, 1 Oct. 2019 - C-673/17, MMR 2019, 732, para. 61 et seq. - Planet49; Podzun, R./Bongartz, P./Kirk, A., DMA, 1st ed 2023, Art. 2 para. 148.

2630 Rec. 42 Regulation (EU) No. 2016/679; European Data Protection Board, Guideline 05/2020 on consent under Regulation 2016/679, para. 13; Podzun, R./Bongartz, P./Kirk, A., DMA, 1st ed 2023, Art. 2 para. 148; Paal, B./Pauly, D. A./Ernst, S., DS-GVO BDSG, 3rd ed. 2021, Art. 4 para. 69.

2631 Podzun, R./Bongartz, P./Kirk, A., DMA, 1st ed 2023, Art. 5 para. 147; see also II. 3. e) cc) (6) on *dark patterns* under the DSA.

2632 Rec. 37 Regulation (EU) 2022/2065.

2633 Podzun, R., DMA, 1st ed 2023, Art. 5(2) para. 10.

(d), (e) GDPR. Accordingly, processing is possible if it is necessary for compliance with a legal obligation to which the controller is subject; to protect the vital interests of the data subject or of another natural person; or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. However, processing pursuant to Art. 6(1)(b) and (f) GDPR is not possible, which leads to a restriction of the rights of the gatekeepers under the GDPR.[2634]

gg) Prohibition of parity clauses, Art. 5(3) DMA

Art. 5(3) DMA standardises a ban on so-called **parity clauses** (or **best price clauses**) for gatekeepers.[2635] This means that gatekeepers are prohibited from using contractual conditions or other measures to prevent commercial users from offering the same products or services to end users via third-party online intermediary services (broad or cross-platform parity clauses) or via their own direct online distribution channels (narrow parity clauses) at different prices or conditions than via the gatekeeper's online intermediary services.[2636] Broad parity clauses further restrict contestability by other platforms and thus the choice of other online intermediary services for end users.[2637] Commercial users should be able to choose freely between the online intermediary services operated by the gatekeeper and other online intermediary services or direct online distribution channels and offer their products or services to end users on differentiated terms.[2638]

hh) Prohibition of anti-steering measures, Art. 5(4) DMA

Article 5(4) DMA prohibits gatekeepers from restricting the freedom of their commercial users**.** Commercial users should therefore be allowed to communicate with their end users outside of the central platform service. Gatekeepers must organise interactions on platforms in such a way that commercial users are free to choose the distribution channel that they consider to have the best attributes for interacting with end users.[2639] Downstream, this should also benefit the end user, as they will be able to choose between the commercial user's offers independently of the respective central platform service.[2640] Art. 5(4) DMA thus also indirectly serves to protect end users' freedom of contract.[2641] The background to the regulation is so-called '**anti-steering' measures**, in which gatekeepers do not allow commercial users to use their central platform service to acquire customers, but then redirect the customers to their own websites or other platforms by using communication content.[2642] In particular, such 'anti-steering

---

2634 Rec.36 Regulation (EU) 2022/2065.
2635 German Federal Court (*BGH), GRUR 2021*, 1213; Podzun, R./Heinz, S., DMA, 1st ed 2023, Art. 5(2) para. 32; MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 116.
2636 Rec. 39 Regulation (EU) 2022/2065; Podzun, R./Heinz, S., DMA, 1st ed 2023, Art. 5(2) para. 32.
2637 Rec. 39 Regulation (EU) 2022/2065.
2638 Rec. 39 Regulation (EU) 2022/2065.
2639 Rec. 40 Regulation (EU) 2022/2065.
2640 Louven, S., 'DMA Art. 5', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 62; Podzun, R./Heinz, S., DMA, 1st ed 2023, Art. 5(4) para. 63.
2641 Louven, S., 'DMA Art. 5', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 62.
2642 Rec. 39 Regulation (EU) 2022/2065.

rules‘ have come to light in antitrust law decisions on ‘app stores‘.[2643] However, Art. 5(4) DMA is formulated broadly in terms of its scope, so that developments in this regard can be dealt with flexibly in the future.[2644] In addition, the provision is intended to reduce the dependency of commercial users on the central platform service. It is also intended to encourage the parallel use of several services (multi-homing).[2645]

ii) Access and use of content acquired elsewhere, Art. 5(5) DMA

Art. 5(5) DMA should allow end users to access content acquired outside the platform. The end user should be able to use digital content, subscriptions, functions or other elements via the gatekeeper's platform even if they were not obtained directly from the gatekeeper. In this way, the behavioural requirement is intended to prevent ‘**lock-in effects‘** and counteract the permanent binding of the end user to the gatekeeper.[2646] The gatekeeper is thus also to be deprived of control over the business relationship between the end user and the commercial user.[2647] In this respect, Art. 5(5) DMA indirectly protects the commercial user with regard to offers outside the respective platform.[2648] The provision is closely linked to Art. 5(4) DMA, although the focus is on the performance of contracts already concluded and not on the initiation of contracts.[2649]

There is no restriction within the standard to specific content or categories of purchased items. The gatekeeper may not base its refusal of access solely on the fact that the content in question was not specifically acquired by it, although Art. 5(5) DMA was formulated in an open manner as to whether access can be restricted for other reasons.[2650] In view of the drafting history, ‘app stores‘ in particular are likely to be covered as addressees of the standard, whereby narrower intermediary services as well as possible future developments may be included.[2651]

jj) Prohibition of obstruction of legal remedies, Art. 5(6) DMA

With Art. 5(6) DMA, the European legislator prohibits gatekeepers from obstructing notifications by users to authorities and national courts due to violations of Union or national law. However, sentence 2 allows internal agreements on complaint and dispute resolution mechanisms between the gatekeeper and commercial users. The provision therefore protects law enforcement against gatekeepers by allowing

---

2643 See, for example, Commission press release of 4 March 2024, available at: https://ec.europa.eu/commission/presscorner/detail/de/ip_24_1161w (last accessed on 1 November 2024); Commission press release of 16 June 2020, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073 (last accessed on 1 November 2024); recommendation for a resolution and report by the Committee on Economic Affairs and Energy (9th Committee), BT-Drs. 19/25868, 115.

2644 Podzun, R./Heinz, S., DMA, 1st ed 2023, Art. 5(4) para. 69.

2645 Rec. 40 Regulation (EU) 2022/2065.

2646 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 161.

2647 Louven, S., ‘DMA Art. 5‘, in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 78.

2648 Podzun, R./Heinz, S., DMA, 1st ed 2023, Art. 5(4) para. 98; MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 160 et seq.

2649 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 160.

2650 Louven, S., ‘DMA Art. 5‘, in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 74.

2651 Podzun, R./Heinz, S., DMA, 1st ed 2023, Art. 5(4) para. 98.

business users and end users to report concerns about unfair practices and infringements to the competent authorities.[2652] The prohibition applies not only to the obligations of the DMA, but also to any infringements of the law, as well as to all practices of the gatekeeper, so that practices relating to other services of the gatekeeper are also covered.[2653] Furthermore, the legal violations do not have to have a direct impact on the user and/or be proven.[2654] As examples of prohibited practices, the DMA mentions discriminatory access conditions, unjustified account blocking of commercial users or unclear reasons for the delisting of products. In addition to the protection of users, Art. 5(6) DMA also ensures the ability of the authorities to work, which require information from complainants, particularly in the context of antitrust proceedings.[2655]

kk) Prohibition of tying central platform services with selected other services, Art. 5(7), (8) DMA

Art. 5(7) DMA standardises a **prohibition of tying**, according to which the use of the central platform service may not be tied to the condition of using other services of the gatekeeper. This applies equally to end users and commercial users, whereby the latter's freedom to choose services other than those of the gatekeeper is to be protected in particular.[2656] Nevertheless, the provision does not create an obligation for the commercial user to offer any alternatives to the end user.[2657] The provision of Art. 5(8) DMA also standardises a prohibition of tying, according to which the gatekeeper is prohibited from tying the use of its central platform service to the registration or subscription of another central platform service. This applies to both end users and commercial users. Such tying mechanisms make it easier for gatekeepers to accumulate data and thus create barriers to market entry.[2658] Thus, Art. 5(8) DMA is intended to ensure the contestability of the central platform services and indirectly protect the freedom of commercial users and end users.[2659] The provision is closely linked to Art. 5(2) DMA, which prohibits the aggregation of data and the mandatory registration of end users with other services, but already applies at an earlier point.[2660]

ll) Right to information, Art. 5(9), (10) DMA

An advertiser's **right to information** from a gatekeeper that provides online advertising services is standardised in Art. 5(9) DMA. Upon request, the gatekeeper must provide the advertiser with information free of charge on a daily basis regarding the adverts placed by the advertiser. The same applies to third parties authorised by the advertiser. The obligation to provide information includes the prices and fees paid by the advertiser (a), the remuneration received from the publisher (b) and the key figures

2652 Rec. 42 Regulation (EU) 2022/2065.
2653 Louven, S., 'DMA Art. 5', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 87.
2654 Louven, S., 'DMA Art. 5', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 88 et seq.
2655 Podzun, R./Heinz, S., DMA, 1st ed 2023, Art. 5(6) para. 121.
2656 Rec. 43 Regulation (EU) 2022/2065.
2657 Rec. 43 Regulation (EU) 2022/2065.
2658 Rec. 44 Regulation (EU) 2022/2065.
2659 Podzun, R./Heinz, S., DMA, 1st ed 2023, Art. 5(8) para. 172.
2660 Louven, S., 'DMA Art. 5', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 109.

on the basis of which the individual prices, fees and remuneration are calculated (c). Art. 5(10) DMA standardises a right to information on the part of the publisher for whom the gatekeeper provides online advertising services. The content of the right to information includes the remuneration received and the fees paid by the publisher, including any deductions and surcharges, for each relevant online advertising service provided by the gatekeeper (a), the price paid by the advertiser, including any deductions and surcharges, subject to the advertiser's consent (b), and the key figures according to which the individual prices and remunerations are calculated (c). The publisher's right to information is essentially similar to that of the advertiser in Art. 5(9) DMA and mirrors the corresponding obligations of the gatekeeper on two different platform markets.[2661] The context of these disclosure obligations is the frequently non-transparent way in which gatekeepers deal with the conditions for their advertising services vis-à-vis commercial users.[2662] The aim is to make it easier for advertisers to switch between individual providers of online advertising services by improving the comparability of conditions. In addition, the costs for online advertising services should also fall.[2663]

Publishers of online advertising services are those who offer the projection surface for advertising, such as the operators of blogs or an online magazine.[2664] This advertising space is often marketed through the use of intermediaries, who in turn offer the advertising space to advertisers.[2665] The brokerage usually takes place on online platforms in the form of an auction.[2666] This platform plays an important intermediary role in the relationship between advertisers and publishers.[2667] If the online platform then also belongs to a gatekeeper, it is usually responsible for controlling access to the users of its platform.[2668]

It is not necessary for the online advertising service itself to be considered a central platform service for the right to information; rather, a certain market strength and affiliation to a gatekeeper is sufficient.[2669] The information must be provided daily and free of charge, whereby a single request for information is sufficient.[2670]

d) Obligations of gatekeepers in accordance with Art. 6 DMA

Art. 6 DMA also standardises directly applicable behavioural requirements for gatekeepers.

mm) Prohibition of data use, Art. 6(2) DMA

Non-publicly accessible data generated or provided by commercial users in the course of using a central platform service may not be used by gatekeepers in competition in accordance with Art. 6(2) DMA. The

2661 Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 5(9) para. 197, 200.
2662 Rec. 45 Regulation (EU) 2022/2065.
2663 Rec. 45 Regulation (EU) 2022/2065.
2664 Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 5(9) para. 201.
2665 Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 5(9) para. 201.
2666 Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 5(9) para. 201.
2667 Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 5(9) para. 205.
2668 Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 5(9) para. 205 with further references.
2669 Louven, S., 'DMA Art. 5', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 109.
2670 Louven, S., 'DMA Art. 5', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 122.

background to this regulation is that gatekeepers often take on a dual role in which they offer a central platform service for commercial users on the one hand and are themselves in competition with these commercial users as providers of competing services or products on the other.[2671] Gatekeepers can use the data collected from commercial users when using the gatekeeper platform in the course of their own service provision on the downstream market and thus optimise their own services. However, they will only make this data available to commercial users to a limited extent, which in turn leads to an information gap and offers potential for abuse.[2672]

The obligation covers all data generated or provided by the business user or its customer, although this does not have to be done on the central platform. Data generated by business users when using the gatekeeper's cloud computing services or its business for software applications via which end users of cloud computing services access software applications is also subject to Art. 6(2) DMA.[2673] If the gatekeeper has generated the data itself and made it available to the business user, without having used data within the meaning of Art. 6(2) DMA, the obligation does not apply.[2674]

With Art. 6(2) DMA, the European legislator is pursuing a more far-reaching approach than the P2BR, which in Art. 7(3)(a) P2BR only provides for a right to information of the commercial user and in Art. 9 P2BR an obligation to provide information in the terms and conditions regarding access to and provision of data to third parties.[2675]

nn) Obligation to uninstall, Art. 6(3) DMA

Art. 6(3) DMA regulates the gatekeeper's obligation to grant authorisation, according to which the gatekeeper is obliged to allow end users to uninstall pre-installed software applications. Although Art. 6(3) DMA does not prohibit the pre-installation as such, it may take the form of such a prohibition if the uninstallation of the programme is not easily feasible for the user.[2676] In exceptional cases, the gatekeeper has the option of restricting **uninstallability** if this is technically necessary. In addition, gatekeepers are also obliged to prevent users from changing the default settings for linked products and services in operating systems, virtual assistants and web browsers (subsection 2). This is to be done by means of a selection field that forces the end user to make an active decision regarding the product or service provider.[2677] The distinction in the subparagraphs between uninstallation and modification options is intended to take account of the special features of the respective services mentioned.[2678] While

[2671] Rec. 46 Regulation (EU) 2022/2065.
[2672] Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 6(2) para. 4 et seq.
[2673] Rec. 48 Regulation (EU) 2022/2065.
[2674] Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 6(2) para. 7.
[2675] Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 6(2) para. 19.
[2676] MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 6 para. 69.
[2677] Flechter, T., DMA Switching Tools and Choice Screens, p. 7.
[2678] Louven, S., 'DMA Art. 6', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para 32.

an operating system can generally be configured as required through individual settings, standard settings such as the online search engine are usually not customised by the end user.[2679] Instead, end users often stick with the default settings that have already been set.[2680] However, this mechanism gives the gatekeeper the opportunity to favour and prefer itself and its services over competing offers through pre-installation.[2681] Art. 6(3) DMA is intended to counteract this.[2682]

oo) Interoperability of software applications and 'app stores', Art. 6(4) DMA

Art. 6(4) DMA contains the obligation of the gatekeeper to enable the installation and use of **software applications** ('apps') and shops for software applications ('**app stores'**) from third-party providers on their operating system. Gatekeepers must also grant them permission and the technical ability to request end users to use their software applications or 'app stores' as the default for corresponding applications. However, the gatekeeper may take measures to maintain the integrity of its operating system (subsection 2) and enable the end user to take protective measures for the security of third-party software applications or 'app stores' (subsection 3). The provision is intended to curb the dominant position of gatekeepers in access to software applications and 'app stores'.[2683] A prominent example of this is 'Apple', against which the Commission recently initiated proceedings to check whether the company complies with the DMA and allows end users to easily uninstall software applications on 'iOS', change the default settings without difficulty and set alternative default services using selection screens.[2684] The provision is intended to benefit both end users and commercial users by allowing them to freely decide whether they want to use third-party services on the gatekeeper's operating system and also to escape the gatekeeper's control through the access path thus opened up.[2685] The provision also favours third-party providers of software applications or 'app stores'.[2686]

pp) Prohibition of self-preferential treatment with regard to rankings, Art. 6(5) DMA

Article 6(5) DMA imposes a strict ban on gatekeepers from favouring themselves in **rankings** as well as in **indexing** and '**crawling'**. 'Crawling' refers to the process in which websites are searched and analysed by a so-called web crawler and then listed on the results page.[2687] This is accompanied by the

---

2679 Podzun, R./Hebers, B., DMA, 1st ed 2023, Art. 6(3) para. 25.
2680 Louven, S., 'DMA Art. 6', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para. 32.
2681 Rec. 49 Regulation (EU) 2022/2065.
2682 Rec. 49 Regulation (EU) 2022/2065.
2683 Rec. 50 Regulation (EU) 2022/2065.
2684 Commission press release of 25 March 2024, available at: https://germany.representation.ec.europa.eu/news/gesetz-uber-digitale-markte-untersuchungen-gegen-alphabet-apple-und-meta-2024-03-25_de (last accessed on 1 November 2024).
2685 Louven, S., 'DMA Art. 6', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para 47.
2686 Schmidt, J.P./Hübener, F./Gasser, L./Hegener, J., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 6 para. 57.
2687 Schmidt, J.P./Hübener, F./Gasser, L./Hegener, J., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 6 para. 58.

indexing process, in which websites are compiled in an organised directory, the index.[2688] The gatekeeper can theoretically put itself in a privileged position during these processes.[2689] Indexing is followed by ranking, which determines the order in which the results are displayed to the user. According to the DMA, any relative emphasis, including the display, assessment, linking or voice output of results falls under the term ranking in accordance with Art. 2(22) DMA. In addition, cases in which the central platform service only displays or communicates a single result to the end user should also be included.[2690] A classic example of such an approach is the presentation of results in online search engines or online marketplaces, although the effect also occurs in other scenarios such as the listing of software applications in 'app stores' or the sorting of videos on video sharing platforms.[2691] The gatekeepers should not favour their products or those offered by a commercial user controlled by them in the ranking on a central platform service or in the associated indexing or *crawling* by legal, commercial or technical means.[2692] In addition, the conditions applicable to such a ranking should generally be fair, transparent and non-discriminatory (Art. 6(5) DMA).

qq) Switching options for end users, Art. 6(6) DMA

Furthermore, gatekeepers may not deny their end users the possibility of switching, either technically or otherwise. End users must be able to switch between or subscribe to software applications and services in accordance with Art. 6(6) DMA. The aim of the provision is to offer more companies the opportunity to provide their services and thus expand the choice of services for end users.[2693] With regard to recital 53 of the DMA, it should be noted that the mere offering of a particular product or service to the end user (e.g. through pre-installation) or the improvement of the offer alone is not to be categorised as a prohibited obstacle to switching providers.

rr) Interoperability of operating systems and virtual assistants, Art. 6(7) DMA

Art. 6(7) DMA regulates a general obligation of the gatekeeper to ensure **interoperability**. In doing so, it must enable the interaction of the services or products offered by service or hardware providers with the hardware and software features of its own operating system or virtual assistant. In addition, they should generally grant commercial users and third-party providers access to the same operating system, software or hardware functions that are available to them for their own offerings. This provision is intended to guarantee end users access to an open internet, as gatekeepers are in a position to technically restrict the end user's effective switch to other companies due to their ability to control hardware or operating systems.[2694] The obligation is intended to give providers of ancillary services the opportunity

[2688] Rec. 51 Regulation (EU) 2022/2065.
[2689] Rec. 52 Regulation (EU) 2022/2065.
[2690] Rec. 52 Regulation (EU) 2022/2065.
[2691] Rec. 51 Regulation (EU) 2022/2065 with further examples.
[2692] Rec. 52 Regulation (EU) 2022/2065.
[2693] Rec. 53 Regulation (EU) 2022/2065.
[2694] Rec. 54 Regulation (EU) 2022/2065.

to compete with the central platform providers.[2695] The practical significance of this regulation can be seen, for example, in the ban on ‘Apple‘ denying ‘Spotify‘ access to the Siri voice assistant (which would allow ,‘iPhone users‘ to play ‘Spotify music‘ by voice command), while ‘Apple Music‘ allows integration with Siri.[2696]

However, the gatekeeper is permitted under Art. 6(7)(2) DMA to take strictly necessary and reasonable measures to protect the integrity of its operating system, virtual assistant, hardware or software function from being compromised by interoperability, subject to the gatekeeper providing sufficient justification for the measures.

ss) Making advertising tools available, Art. 6(8) DMA

In addition, the gatekeeper must make performance measurement tools and other data required for its own independent review of the advertising inventory available to advertisers and publishers, as well as any commissioned third parties, free of charge upon request. This should make the conditions under which gatekeepers provide online advertising services more transparent in future.[2697] The advertising services provided by the gatekeepers and their effectiveness should also become more comprehensible and comparable for the competition.[2698] The obligation under Art. 6(8) DMA is therefore related to the content of the information claims under Art. 5(9) and (10) DMA.[2699] The information provided by the gatekeeper must be designed in such a way as to ensure compatibility with the verification mechanisms and measurement tools of advertisers and publishers (Art. 6(8) DMA).

tt) Obligations to provide access to data, Art. 6(9), (10), (11) DMA

With Art. 6(9) DMA, the European legislator introduces an obligation for gatekeepers to provide end users with access to the data obtained in connection with the central platform service free of charge upon request. All data provided by the end user or generated through the use of the central platform service falls under the obligation to provide access. The data should be made available in a format that the user can access directly and effectively and that is suitable for further use.[2700] Measures for effective usability, such as the provision programme interfaces, should also be taken by the gatekeepers.[2701] The regulation is intended to prevent gatekeepers from undermining the contestability of central platform services or the innovation potential of a dynamic digital sector.[2702] End users should be able to transmission their own data to other platforms and use it there, and it should be possible to switch to other providers and

---

2695 Schmidt, J.P./Hübener, F./Gasser, L./Hegener, J., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 6 para. 68.
2696 Belloso, R., The EU Digital Markets Act, p. 2.
2697 Rec. 58 Regulation (EU) 2022/2065.
2698 Rec. 58 Regulation (EU) 2022/2065.
2699 Schmidt, J.P./Hübener, F./Gasser, L./Hegener, J., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 6 para. 69.
2700 Rec. 59 Regulation (EU) 2022/2065.
2701 Rec. 59 Regulation (EU) 2022/2065.
2702 Rec. 59 Regulation (EU) 2022/2065.

use different services ('multi-homing').[2703] In turn, gatekeepers and commercial users should be incentivised to innovate.[2704]

Art. 6(10) DMA also grants commercial users and third parties authorised by them a right of access within the meaning of Art. 6(9) DMA. The commercial user may also request access to the end user's data that commercial users receive via the central platform service. However, sentence 2 is to be used as a barrier, which only allows such a claim with regard to personal data if the data is directly related to the end user's use of the products or services offered by the commercial user via the central platform service. In addition, the end user must have consented to the disclosure.

Furthermore, according to Art. 6(11) DMA, the gatekeeper is obliged to grant third-party providers of online search engines access to ranking, enquiry, click and view data relating to unpaid and paid search results generated by end users via its online search engines upon request. Access to the data must be granted in compliance with **FRAND conditions**, i.e. on '*fair, reasonable and non-discriminatory*' terms.[2705] If the data contains personal data, the gatekeeper is subject to an anonymisation obligation (Art. 6(11) DMA), whereby the anonymisation should not affect the quality or usability of the data.[2706] Adequate anonymisation can be assumed if the data has undergone such a change that the information can no longer be used to draw conclusions about an identified or identifiable person or the personal data has been anonymised in such a way that the data subject cannot or can no longer be identified. [2707] Data access is intended to give competitors of the gatekeeper the opportunity to improve their own search services through training with the data provided, to strengthen their role on the market and thus overcome any barriers to market entry.[2708]

The obligations to enable **data portability** under Art. 6(9) DMA and to create data access (Art. 6(10), (11) DMA) are closely related to the other provisions of the DMA. Together with the prohibition of data merging (Art. 5(2) DMA), the prohibitions of service coupling (Art. 5(7), (8) DMA) and the obligations of gatekeepers to ensure interoperability (Art. 6 (4), (7) DMA), they are intended to promote access and the transmission or sharing of data and at the same time restrict gatekeepers in their ability to collect and merge data.[2709]

uu) Access for commercial users under FRAND conditions, Art. 6(12) DMA

Art. 6(12) DMA contains the obligation of gatekeepers to guarantee access for commercial users to '*app stores*', online search engines and online services of social networks that have been designated as central platform services by the EU Commission by applying **FRAND conditions**. However, the provision only

---

2703 Podzun, R./Wolf-Posch, A., DMA, 1st ed 2023, Art. 6(9) para. 179 with further references.
2704 Rec. 59 Regulation (EU) 2022/2065.
2705 Rec. 61 Regulation (EU) 2022/2065; Louven, S., 'DMA Art. 6', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para 175.
2706 Rec. 61 Regulation (EU) 2022/2065.
2707 Rec. 61 Regulation (EU) 2022/2065.
2708 Rec. 61 Regulation (EU) 2022/2065.
2709 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 6 para. 205 mwN.

obliges compliance with fair, reasonable and non-discriminatory access conditions, but does not standardise an independent right of access.[2710] This obligation is intended to restrict the gatekeeper's dominant negotiating position as an important access gateway for commercial users to end users.[2711]

The gatekeeper is also obliged to publish the general access conditions in accordance with the provisions of (12) DMA. This is intended to give commercial users the opportunity to gather impressions of the access conditions and make decisions based on these.[2712] By also making the access conditions available for public inspection, alternative providers also have the opportunity to stand out from the competition by offering different access conditions.[2713] The publication must also include a Union-based alternative dispute resolution mechanism. According to recital 62 DMA, this must be easily accessible, impartial, independent and free of charge for commercial users. Furthermore, measures must be provided to prevent abuse of the mechanism. However, the dispute mechanism must not restrict the commercial user's right to seek redress in accordance with Union and national law. The EU Commission is responsible for verifying compliance with the obligations of Art. 12(12) DMA when publishing the general access conditions in accordance with Art. 12(12)(3) DMA.

vv) Terms of cancellation, Art. 6(13) DMA

Art. 6(13) DMA stipulates the prohibition of disproportionate conditions for the cancellation of the use of central platform services or the deletion of an account by the end user or commercial user. In addition, according to Art. 6(13) DMA, the gatekeeper is obliged to ensure that compliance with the cancellation conditions is possible without undue difficulty. This includes, for example, the form of cancellation, the notice period or the reasons for cancellation.[2714] It should be just as easy for the user to cancel a subscription or delete their profile as it is to open an account.[2715] Furthermore, cancellation should not be associated with additional costs for the user.[2716] This provision should also make it easier for users to switch to other services.[2717] Unfair cancellation barriers allow gatekeepers to charge higher prices or reduce the quality of their products without losing users to other services.[2718] This is to be counteracted.

ww) Further obligations

Art. 7 DMA ties in with the gatekeeper's duty of **interoperability** standardised in Art. 6(7) DMA. However, the provision focuses on interpersonal communication services that are not linked to a mobile phone number. This refers in particular to messenger services. At least with regard to the basic functions, the gatekeeper must fulfil the interoperability obligation free of charge by offering the necessary tech-

2710 Rec. 62 Regulation (EU) 2022/2065.
2711 Louven, S., 'DMA Art. 6', in: BeckOK Informations- und Medienrecht (45th ed. 2024) para 175.
2712 Rec. 62 Regulation (EU) 2022/2065.
2713 Louven, S., 'DMA Art. 6', in: BeckOK Informations- und Medienrecht (45th ed. 2024) 192.
2714 Rec. 63 Regulation (EU) 2022/2065.
2715 Rec. 63 Regulation (EU) 2022/2065.
2716 Rec. 63 Regulation (EU) 2022/2065.
2717 Rec. 63 Regulation (EU) 2022/2065.
2718 Kersting, C./Podszun, R./Grave, C., Die 9. GWB-Novelle, 1st ed. 2017, Chapter 2, para. 40.

nical interfaces or similar solutions. According to Art. 7(2) DMA, the implementation of the interoperability obligation must be made possible immediately after the gatekeeper has been designated and includes, for example, end-to-end text messages and the exchange of images, voice messages, videos and other attached files between two individual end users. For the more complex specifications for group messages (b) or video and voice calls, the DMA provides for gradual implementation.

Art. 14 DMA also **requires gatekeepers to inform** the Commission of any mergers. With regard to consumer profiling, gatekeepers must provide the Commission with a description of the techniques used in accordance with Art. 15 DMA.

The obligations of the DMA are exhaustive in nature and no general clause can be used.[2719] However, the Commission has the option, by means of a market investigation with Art. 19(3) DMA, to make additions to individual behavioural obligations or to supplement the DMA with further obligations for gatekeepers by means of a legislative proposal.

4. Supervision and enforcement, Art. 20–43 DMA

Public enforcement of the DMA is the responsibility of the European Commission (**Public Enforcement**).[2720] According to Art. 37, 38 DMA, national authorities should only provide limited support. In addition, the obligations of the DMA can also be enforced under civil law **(private enforcement)**. The DMA's enforcement concept also focuses on **compliance requirements** and regular reporting obligations for gatekeepers.[2721] The gatekeeper must implement the obligations of the DMA independently by amending the GTC, changing the platform design and modifying algorithms. This so-called ***compliance by design approach***, which is already an integral part of the GDPR (Art. 25) or the DSA (Art. 31), is now also to find its way into economic platform regulation through the DMA.[2722] Gatekeepers must demonstrate compliance with the obligations pursuant to Art. 8(1); Art. 13(3) DMA. A comprehensive prohibition of circumvention is standardised by Art. 13(4) DMA. In addition, the gatekeepers are obliged to set up a compliance unit, which must be equipped with extensive powers and resources in accordance with Art. 28 DMA, ensure compliance with the DMA and be available to the Commission as a point of contact. Furthermore, pursuant to Art. 11 DMA, a so-called **compliance report** must be issued by the gatekeeper in both confidential and non-confidential, public form, which provides information on the measures taken to comply with the provisions of the DMA. The scope of such a report is set out in the

2719 Podszun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3253).
2720 Rec. 91 Regulation (EU) 2022/2065.
2721 Schmidt, J.P./Hübener, Das neue Recht der digitalen Märkte, 1st ed. 2023, § 7 para. 1.
2722 Taeger, J./Pohle, T./Podszun, R./Kirk, A., Computerrechts-Handbuch, 39 th ed. 2024, Part 12 120.3 Digital Markets Act, para. 64.

template published by the Commission.[2723] According to this, any changes to the user experience, technical changes, A/B tests and information on indicators that can be used to measure the effectiveness of compliance measures with regard to the objectives of the DMA must be reported.[2724] In their compliance reports published at the beginning of March 2024, the companies previously appointed as gatekeepers addressed the requirements of the DMA to varying degrees and with varying degrees of detail.[2725]

a) Public Enforcement

In the event of non-compliance, the EU Commission can use various sanction mechanisms and a wide range of investigative powers to enforce the DMA. It is therefore particularly important for practitioners to know the relevant requirements and legal protection options in order to best protect their own interests.

If a gatekeeper violates the provisions of the DMA, the Commission shall issue a non-compliance decision pursuant to Art. 29 DMA requesting the gatekeeper to cease non-compliance within a reasonable period of time and to explain what measures it will take to comply with this decision. Before doing so, the Commission must inform the gatekeeper concerned of the future steps that it intends to take or that the gatekeeper should take. Such proceedings for non-compliance with the DMA were initiated by the Commission on 25 March 2024 against the gatekeepers '*Alphabet', 'Apple'* and '*Meta'* for possible violations of Art. 5(2), (4) DMA and Art. 6(3), (5) DMA.[2726]

b) Sanction options, Art. 20 et seqq. DMA

In its non-compliance decision, the Commission can also specify corresponding penalties. Despite the Member States' right of initiative, the Commission has the sole right to impose such sanctions (Art. 38(7) DMA). In the event of infringements, it can impose fines in accordance with Art. 30 DMA or periodic penalty payments in accordance with Art. 31 DMA. The Member States only have the option of resorting to national sanction mechanisms under competition law.[2727] The fine is imposed by the Commission for a past infringement of the DMA, whereas the periodic penalty payments are imposed with a view to future compliance with the DMA. If there is a system behind the gatekeeper's non-compliance, Art. 18 DMA also allows the Commission to resort to further behavioural or even structural remedies such as the prohibition of mergers. Furthermore, the Commission can impose interim measures in accordance with Art. 24 DMA.

2723 European Commission, Template Form for Reporting pursuant to Article 11 of Regulation (EU) 2022/1925 (Digital Markets Act) (Compliance Report), available at: https://digital-markets-act.ec.europa.eu/document/download/904debdf-2eb3-469a-8bbc-e62e5e356fb1_en?filename=Article%2011%20DMA%20-%20Compliance%20Report%20Template%20Form.pdf (last accessed on 1 November 2024).

2724 Taeger, J./Pohle, T./Podszun, R./Kirk, A., Computerrechts-Handbuch, 39 th ed. 2024, Part 12 120.3 Digital Markets Act, para. 65.

2725 Taeger, J./Pohle, T./Podszun, R./Kirk, A., Computerrechts-Handbuch, 39 th ed. 2024, Part 12 120.3 Digital Markets Act, para. 65.

2726 Commission press release of 25 March 2024, available at: https://ec.europa.eu/commiasion/presscorner/detail/de/ip_24_1689 (last accessed on 1 November 2024).

2727 Schmidt, J.P./Hübener, F./Reims, R., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 10 para. 3.

aa) Order to pay a fine, Art. 30 DMA

The amount of the fine is determined on the basis of the gatekeeper's total turnover in the previous financial year and can amount to up to 10% of this turnover in the event of a substantive offence and up to 20% in the event of a repeat offence. In the event of a formal offence, a fine of up to 1% of the turnover to be determined is to be expected. The amount of the fine in detail is determined in accordance with Art. 30(4) DMA according to the severity, duration and repetition of the infringement, whereby recourse to the pronounced antitrust practice is also to be expected here.[2728] A fine can also be imposed on companies or associations of companies that have not assumed a gatekeeper position in the event of formal violations of the DMA (provided they were committed negligently or intentionally). The question so far is the relationship between the imposition of fines under the DMA on the one hand and antitrust law on the other for the same behaviour and whether this constitutes a violation of the prohibition of double jeopardy ('ne bis in idem') standardised in Art. 50 CFR.[2729] In principle, there is nothing to prevent the cumulative imposition of fines under the DMA and antitrust law in view of the different objectives.[2730] In the opinion of the European Court of Justice, double prosecution must nevertheless be taken into account to reduce the fine.[2731]

bb) Penalty payments, Art. 31 DMA

The amount of the periodic penalty payments is determined by the average worldwide daily turnover achieved in the previous financial year. Art. 31 DMA is preventive in nature and therefore also applies in the absence of fault on the part of the addressee of the periodic penalty payment.[2732] If the company fulfils the obligation, the EU Commission can set the final amount of the periodic penalty payment at a lower amount than the amount originally set by the decision in accordance with Art. 31(2) DMA.

cc) Systematic non-compliance, Art. 18 DMA

Further measures in the event of systematic non-compliance in accordance with Art. 18 DMA require a market investigation, in which the gatekeeper concerned is notified of the objections and the intended remedial measures within six months of the initiation of the investigation in accordance with Art. 18(1) DMA. According to Art. 18(1) DMA, the result of the market investigation must be systematic non-compliance with one or more of the obligations set out in Art. 5, 6 or 7 DMA and a strengthening of the gatekeeper's position with regard to the criteria set out in Art. 3(1) DMA. Non-compliance is automatically assumed pursuant to Art. 18(3) DMA if the Commission imposes at least three non-compliance decisions within eight years prior to the initiation of a market investigation. If these conditions are met, the EU Commission can order any behavioural or structural remedial measure against the gatekeeper

---

2728 Schmidt, J.P./Hübener, F./Reims, R., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 10 para. 14.

2729 Federal Cartel Office (Bundeskartellamt), Background Paper DMA p. 42; Schmidt, J.P./Hübener, F./Reims, R., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 10 para. 19.

2730 Harta, J., cepInput No. 12/2021, p. 10.

2731 Schmidt, J.P./Hübener, F./Reims, R., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 10 para. 22 with further references; Harta, J., cepInput No. 12/2021, p. 10.

2732 Schmidt, J.P./Hübener, F./Reims, R., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 10 para. 23, 24.

that is appropriate and necessary to comply with the requirements of the DMA in accordance with Art. 18(1) DMA.

dd) Provisional measures, Art. 24 DMA

Finally, in urgent cases, the Commission has the option of taking interim measures against the gatekeeper pursuant to Art. 24 DMA. This requires the establishment of a 'prima facie' infringement of Art. 5, 6 or 7 DMA and the risk of serious and irreparable harm to commercial users or end users. However, the order is only admissible in the context of proceedings initiated with a view to the possible issuance of a non-compliance order pursuant to Art. 29(1) DMA.

ee) Investigative powers of the European Commission, Art. 21 et seq. DMA

Furthermore, the EU Commission has a number of investigative powers under Art. 21 et seq. of the DMA. It can exercise these powers even before initiating proceedings on the possible adoption of a non-compliance decision, Art. 20(2) DMA. In accordance with Art. 21 DMA, the Commission can request the relevant companies to provide all necessary information by means of a simple request for information or by way of a decision. This also includes access to all data and algorithms of companies and information on tests as well as related explanations. In addition, pursuant to Art. 21(5) DMA, it may also make a request for information to the authorities of the Member States. Furthermore, pursuant to Art. 22 DMA, the Commission may question any natural or legal person and record such questioning by any technical means, provided that the person consents to the questioning for the purpose of obtaining information relating to the subject matter of an investigation. The Commission is also responsible under Art. 23 DMA for carrying out inspections to fulfil its duties under the DMA. In doing so, the Commission officials responsible for the inspections and other accompanying persons authorised by the Commission are authorised to enter all premises, examine the books and other business documents, make or request copies or extracts thereof, seal business premises and books or documents to the extent necessary for the duration of the inspection, as well as request explanations of facts or documents and record the answers by technical means.

c) Private enforcement

In addition to the official enforcement of the provisions of the DMA, there is also the possibility of **private enforcement**. Although the DMA does not contain any explicit provisions on private enforcement,[2733] it gives competitors, commercial users or end users the opportunity to enforce obligations under the DMA in negotiations with the gatekeepers by lodging complaints with the Commission or taking legal action and, if necessary, claiming damages.[2734] **Private enforcement** is based on European law, where it is already common practice that European law also gives rise to individual rights of individuals,

[2733] Schmidt, J.P./Hübener, F./Schläfke, H./Schuler, I., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 13 para. 1.

[2734] Podszun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3253) mwN.

which act as a further effective check on the protection of their rights by way of individual enforcement.[2735] It is also clear from Art. 39 and 42 DMA that the possibility of private enforcement should also exist.[2736] Art. 39 DMA regulates the co-operation of the Commission with national courts, whereby the national courts are bound by the decisions of the Commission. The possibility of private enforcement arises from the fact that national civil proceedings can rule on the provisions of the DMA.[2737] Art. 42 DMA declares the Consumer Associations Directive[2738] and thus private collective redress applicable within the framework of the DMA.[2739] Enabling private enforcement has many advantages: on the one hand, the EU Commission can be relieved of the burden of enforcing the DMA and, on the other, private enforcement offers a differentiated perspective.[2740] Cases can be dealt with in a decentralised manner so that different market conditions in the various member states can be taken into account in the assessment.[2741] In addition, the focus is on the individual perspective of plaintiffs.[2742]

ff) Requirements for enforcement under private law and applicable regulations

As such, the DMA is primarily aimed at gatekeepers. In order for users or other competitors to be able to invoke the provisions of the DMA, they must be directly applicable.[2743] In principle, the DMA is already generally and directly applicable in the Member States due to its nature as a regulation pursuant to Art. 288(2) TFEU. In order to trigger rights for individuals and thus be the subject of private enforcement, the relevant standard must be sufficiently specific in the individual case.[2744] The decisive factor here is whether the implementation of the respective standard is necessarily linked to further measures by the Union institutions or the Member States or whether it is a self-executing provision, i.e. applicable on its own.[2745] At the same time, the specificity of the content must result in corresponding individual protection so that the provision can be enforced by the individual before the national courts.[2746] Against this background, the obligations standardised in Art. 5 DMA are particularly suitable, as they do not require any concretisation by the Commission.[2747] In addition, the obligations in Art. 6 and 7 DMA are also suitable; here, too, the Commission is not required to specify them.[2748] The other provisions of the

---

2735 Schmidt, J.P./Hübener, F./Schläfke, H./Schuler, I., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 13 para. 2 with further references.
2736 Podzun, R./Lahme, R. /Ruster, A., DMA, 1st ed 2024, Art 39 para. 1.
2737 Galle, R./Dressel, F., *EuZW* 2024, 107 (107).
2738 Directive (EU) 2020/1828.
2739 MüKoEuWettbR/Voell, B., 4th ed. 2024, DMA Art. 42 para. 2.
2740 Galle, R./Dressel, F., *EuZW* 2024, 107 (107).
2741 Galle, R./Dressel, F., *EuZW* 2024, 107 (108).
2742 Galle, R./Dressel, F., *EuZW* 2024, 107 (108) et seq.
2743 Schmidt, J.P./Hübener, F./Schläfke, H./Schuler, I., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 13 para. 4.
2744 Streinz, R./Schroeder, W., EUV/AEUV, 3rd ed. 2018, Art. 288 para. 91.
2745 Komninos, A., FS Fox, 2021, 425, 428.
2746 Schmidt, J.P./Hübener, F./Schläfke, H./Schuler, I., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 13 para. 5, with further references.
2747 Podszun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3253).
2748 Podszun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3253).

DMA are mainly of a procedural nature and concern the application of the DMA by the Commission, which is why the question of direct effect does not generally arise here.[2749]

gg) Practical relevance of private enforcement

The enforcement of the DMA under private law is likely to become particularly relevant in connection with urgent legal protection.[2750] This is illustrated by the EU Commission's commitment decision of 20 December 2022, in which action was still taken against Amazon under traditional EU competition law.[2751] Amazon's behaviour, which was criticised at the time the proceedings were opened in July 2019 and November 2020, had already been under fire for many years.[2752] Until the commitment becomes binding at the end of June 2023, it can be assumed that the affected parties have suffered considerable harm, which could have been counteracted at an early stage by means of a private (urgent) enforcement of removal and injunctive relief claims on the basis of an already applicable DMA (Art. 6(2), (5) DMA).[2753] Particularly for commercial users and competitors, the assertion of rights under the DMA by way of a (civil) action can therefore bring advantages, despite the risk of cost-intensive and lengthy proceedings.[2754] In view of the fast-moving digital sector, facts can be established at an early stage and irretrievable damage caused by gatekeeper practices can be avoided.[2755]

It is to be expected that the enforcement of the DMA under private law will be of considerable practical importance.[2756] However, in view of the lack of relevant DMA case law, practitioners will be confronted with both substantive and procedural issues.[2757] Examples include international jurisdiction and the applicable law in cross-border disputes as well as the civil law obligation to provide evidence of an infringement.[2758]

5. Summary and implications for practice

For gatekeepers, many of the DMA's provisions are associated with significant interference in their business models.[2759] Since March 2024, companies already designated as gatekeepers must comply with the prohibitions and restrictions for their central platform services and fulfil the objectives of the DMA by taking appropriate measures (Art. 8(1) DMA). In this context, it is relevant that companies can avoid being designated as gatekeepers by providing appropriate invalidating arguments (Art. 3(5) DMA). To date, the Commission's main focus has been on examining whether companies have implemented the

---

2749 Komninos, A., FS Fox, 2021, 425, 429.
2750 Galle, R./Dressel, F., *EuZW* 2024, 107 (108); Podszun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3253).
2751 COM(2022) 9442 final - *Case AT.40462 - Amazon Marketplace and Case AT.40703 - Amazon Buy Box*.
2752 Richter, A./Gömann, M., *NZKart* 2023, 208 (208) mwN.
2753 Richter, A./Gömann, M., *NZKart* 2023, 208 (208).
2754 Podszun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3253).
2755 Podszun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3253).
2756 Schmidt, J.P./Hübener, F./Schläfke, H./Schuler, I., Das neue Recht der digitalen Märkte, 1st ed. 2023, § 13 para. 1.
2757 Podszun, R./Bongartz, P./Kirk, A., *NJW* 2022, 3249 (3253) et seq.
2758 See in detail, for example, Becker, B, *ZEuP 2023*, 403; Richter, A./Gömann, M., *NZKart* 2023, 208 (208).
2759 Hebers, B., *BB 2022*, I (I).

obligations of the DMA in principle, and initial proceedings against violations have already been initiated.[2760]. Even though the DMA primarily addresses gatekeepers and therefore only primarily obliges a very small number of large corporations such as ‘Amazon‘, ‘Apple‘, ‘Meta‘ or ‘Microsoft‘, smaller companies are also affected by the DMA. They can also benefit from the DMA's objective of creating fair and contestable digital markets. As commercial users, competitors or end users, they can proactively inform the Commission of infringements by gatekeepers in accordance with Art. 27 DMA and thus initiate proceedings by the Commission or national competition authorities. The DMA also offers affected parties the opportunity to comment on planned compliance measures by gatekeepers (Art. 8(6) DMA) or in connection with market investigations due to systematic non-compliance or in relation to new services or practices (Art. 18(5), (6) DMA or Art. 19(2) DMA). Last but not least, those affected can also take legal action against the gatekeepers by way of private enforcement before courts in the Member States. In order to be able to act accordingly, it is essential for competitors and users to familiarise themselves with the regulations of the DMA, despite the lack of gatekeeper status.

a) Criticism regarding the appointment of gatekeepers

In order to justify the designation as a gatekeeper, the qualitative requirements of Art. 3(1) DMA must be met. This includes a significant influence of the company on the internal market as well as the provision of a central platform service that serves commercial users as an important gateway to end users. In addition, the company must have a consolidated and permanent position with regard to its activities or achieve such a position in the foreseeable future (c). On the other hand, the Commission can also use the quantitative criteria standardised in Art. 3(2) DMA to determine a gatekeeper position. The gatekeeper status is assumed on the basis of size characteristics such as turnover, market capitalisation and the number of monthly users. Pursuant to Art. 3(3) DMA, a company whose central platform service exceeds the quantitative thresholds specified in Art. 3(2) DMA is obliged to inform the Commission of this fact immediately, but at the latest within two months. The Commission must then designate the company as gatekeeper within 45 working days. The potential gatekeeper will be subject to this obligation if it has more than 45 million monthly active users, although only private users count and at least 10,000 commercial users are also required. The user number limits apply to the company's individual platform service. Difficulties arise with regard to the delimitation of the individual platform services, especially if the platform offers different services for different user groups, such as buying, selling and renting cars.[2761] Ambiguities also arise in the case of additional services offered.[2762] Although the annex to the DMA is intended to provide assistance with such questions, it does not have any legal effect[2763]

[2760] Commission press release of 24 June 2024, available at: https://germany.representation.ec.europa.eu/news/verstoss-gegen-gesetz-uber-digitale-markte-eu-kommission-leitet-untersuchung-gegen-apple-ein-2024-06-24_de (last accessed on 1 November 2024).

[2761] Küster, S., BB 2022, 2819, 2820.

[2762] Küster, S., BB 2022, 2819, 2820.

[2763] No. 1, Annex to Regulation (EU) 2022/2065.

and only provides limited information on the above-mentioned problem.[2764] However, in cases where a core product is equipped with other complementary products or services, thus creating a digital ecosystem, it is more likely to be an important gateway to end users.[2765] Due to the high level of regulation, the DMA must generally be applied strictly, especially as ambiguities or uncertainties regarding the fulfilment of individual thresholds can be discussed with the Commission prior to notification in accordance with Art. 3(3) DMA and, depending on the outcome, a notification can also be refrained from.[2766]

In addition, pursuant to Art. 3(5)(2) DMA, the company concerned can demonstrate in its notification that the **quantitative thresholds** of Art. 3(2) DMA do not create a gatekeeper status in the specific case. In this respect, Art. 3(2) DMA is designed as a rebuttable presumption and is intended to make it easier to prove that the requirements for gatekeeper status are met.[2767] However, the extent to which the relevant company must counter the presumption of Art. 3(2) DMA is a difficult endeavour. Due to reaching the thresholds, 'Alphabet', 'Amazon', 'Apple', 'ByteDance', 'Meta', 'Microsoft' and 'Samsung' fulfilled their notification obligation as potential gatekeepers on 3 July 2023,[2768] but at the same time all companies argued against their appointment as gatekeepers.[2769] Success was achieved in three cases, meaning that no appointment as gatekeepers was made and the Commission also refrained from initiating a market investigation pursuant to Art. 16(1) in conjunction with Art. 17(1) DMA.[2770] In four other cases, the presumption of conformity pursuant to Art. 3(2) DMA was successfully rebutted, but a market investigation was initiated for further assessment in each case.[2771] With the exception of 'Samsung', all companies were unsuccessful in rebutting the presumption of conformity and were at least found to be operating one or more centralised platform services.[2772] It is problematic in that the Commission refrains from providing clarification in its findings and does not explain which of the arguments put forward sufficiently substantiates the rebuttal of the presumption of conformity.[2773] In particular, no stringent line of argumentation on the part of the Commission can be recognised.[2774] While in the course of the proceedings against 'ByteDance' it considered the lack of 'lock-in effects' of end users and commercial users due to a lack of network effects to be insufficient,[2775] similar arguments were taken into account

2764 Küster, S., *BB 2022*, 2819, 2822.
2765 Higer, D./Patt, C., *NZKart* 2024, 78 (79) et seq.
2766 Higer, D./Patt, C., *NZKart* 2024, 78 (81).
2767 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 3 para. 46.
2768 COM(2024) 106 final, p. 2.
2769 Kleine, M./Mienert, D./Moryn, K./Timm, O., News Service Compliance 2024, 220008.
2770 COM(2023) 6106 final, *Microsoft - number-independent interpersonal communications services (NIICS)*, para. 134; COM(2023) 6101 final, DMA.100006 - *Alphabet - NIICS*, para. 150; COM(2023) 6103 final, DMA.100038 - *Samsung - web browsers*, para. 50.
2771 COM(2023) 6078 final, DMA. 100015 - *Microsoft - online search engines*, para. 14 et seq.; COM(2023) 6077 final, DMA.100022 - *Apple - NIICS*, para. 12; COM(2023) 6078 final, DMA.100034 - *Microsoft - online advertising services*, para. 14 et seq.; COM(2023) 6078 final, DMA.100028 - *Microsoft - web browsers*, para. 14 et seq.
2772 Kleine, M./Mienert, D./Moryn, K./Timm, O., News Service Compliance 2024, 220008.
2773 Higer, D./Patt, C., *NZKart* 2024, 78 (84).
2774 Higer, D./Patt, C., *NZKart* 2024, 78 (84).
2775 COM(2023) 6102 final, DMA.100040 - *ByteDance - Online social networking services*, para. 103.

in the assessment of the ‘Samsung Web Browser‘, ‘Microsoft Outlook‘ and ‘Gmail‘.[2776] ‘ByteDance‘ also argued with the relative size of ‘TikTok‘ compared to other social networks.[2777] The Commission also considered this to be unconvincing,[2778] even though the argument was used in the case of ‘Gmail‘ and ‘Outlook‘ in favour of non-designation.[2779] Consequently, such contradictions in the Commission's practice result in significant legal uncertainties.[2780]

b) Criticism regarding the prohibition of data merging (Art. 5(2) DMA)

The prohibition of data merging in Art. 5(2) DMA has also been criticised.[2781] This relates in particular to the requirement for consent, the practical effectiveness of which is being questioned, especially with regard to the regulatory objectives of the DMA.[2782] It can be assumed that end users are often unable to understand the extent of their consent and therefore de facto authorise the processing of their personal data without further ado.[2783] In addition, gatekeepers can more easily obtain the consent of users through their seductive skills in practice and through appropriate design and thus utilise their data power.[2784] However, if the user refuses consent instead, the deniability is torpedoed at the same time.[2785]

c) Outlook

However, whether the DMA has further weaknesses and in what form they occur will only be revealed in the future through more experience with the handling of the DMA by the Commission as well as by the gatekeepers themselves. In view of their extensive financial and human resources, it is quite conceivable that the gatekeepers will successfully prevail against the Commission and an overly harsh cutback in their previous approach.[2786] At the same time, the rapid initiation of proceedings against ‘Apple‘, ‘Meta‘ and ‘Alphabet‘ indicates that the Commission will take decisive action in the event of any violations of the DMA.[2787] These proceedings and any pending lengthy proceedings before the European Court of Justice also allow conclusions to be drawn about the practicability of the DMA.[2788] In addition, the global activities of the gatekeepers should not be neglected, which could also lead to stronger regulation of large digital groups in other European countries in the future, modelled on the legislation here.[2789]

2776 COM(2023) 6103 final, DMA.100038 - *Samsung - web browsers*, para. 45 et seq.; COM(2023) 6106, DMA.100006 - *Alphabet - NIICS*, para. 145; COM(2023) 6106 final, *Microsoft -NIICS*, para. 129.

2777 COM(2023) 6102 final, DMA.100040 - *ByteDance - Online social networking services*, para. 103; ByteDance had lodged an appeal against the Commission's decision. However, the EGC has since dismissed the action for annulment and classified Bytedance as a gatekeeper, *EGC*, 17 Jul. 2024- T-1077/23.

2778 COM(2023) 6102 final, DMA.100040 - *ByteDance - Online social networking services*, para. 163.

2779 Higer, D./Patt, C., *NZKart* 2024, 78 (84).

2780 Higer, D./Patt, C., *NZKart* 2024, 78 (84).

2781 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 111.

2782 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 111, with further references.

2783 MüKoEuWettbR/Bueren, E./Weck, T., 4th ed. 2024, DMA Art. 5 para. 111.

2784 Kerber, W., *ZD* 2021, 544 (546).

2785 Podzun, R., *GRUR Int.* 2022, 197 (199).

2786 Hegener, J.C., *RDi* 2024, 267, 275 et seq.

2787 Hegener, J.C., *RDi* 2024, 267, 275 et seq.

2788 Drewes, H./Meyer, L./Moss, P., *RDi* 2024, 310 (314).

2789 Kleine, M./Mienert, D./Moryn, K./Timm, O., News Service Compliance 2024, 220008.