Schreiber / Pommerening / Schoel

New Data Act

A Practitioner's Guide

Schreiber / Pommerening / Schoel

New Data Act

New Data Act

A Practitioner's Guide

by

Kristina Schreiber
Patrick Pommerening
Philipp Schoel

2026

Published by
Nomos Verlagsgesellschaft mbH & Co. KG, Waldseestraße 3-5, 76530 Baden-Baden, Germany,
email: service@nomos.de

Co-published by
Verlag C.H.Beck oHG, Wilhelmstraße 9, 80801 München, Germany,
email: bestellung@beck.de

and

Hart Publishing, Kemp House, Chawley Park, Cumnor Hill, Oxford, OX2 9PH, United Kingdom,
online at: www.hartpub.co.uk

Published in North America by Hart Publishing,
An Imprint of Bloomsbury Publishing 1385 Broadway, New York, NY 10018, USA
email: mail@hartpub.co.uk

ISBN 978 3 7560 0991 6 (NOMOS Print)
ISBN 978 3 7489 4949 7 (NOMOS ePDF)
ISBN 978 3 406 83136 2 (C.H.BECK)
ISBN 978 1 5099 8494 7 (HART)

First Edition 2026

Preface

The EU's Digital Strategy gathered pace. In recent years, a large number of new 'Digital Acts', generally EU regulations, have been submitted in draft form or have already been adopted. As a central pillar of the Data Strategy, which is part of the EU's digital agenda, the Data Act (DA) has been published in the Official Journal of the EU and marks a new chapter for the European data economy. Most of its rights and obligations have become applicable on 12.9.2025.

A radical change has been under discussion since November 2025 at the latest: The Digital Omnibus on digital acquis, the Commission's proposal for a new regulation that will change several digital acts, is intended to streamline and reduce bureaucracy. However, the Commission's proposal envisages even a significant strengthening of the Data Act: It will remain at the centre of data economy regulation and is even to be expanded to incorporate several other legal acts in the future. This clearly demonstrates the central role that this legal act will continue to play in the EU's digital regulation.

From the EU's perspective, the Data Act contains key instruments to strengthen access to and use of data across the internal market, aiming to enable fairer allocation of value and broader innovation opportunities. The focus is notably on data generated by connected products, on enhancing data accessibility for users, on clarifying data usage rights, and on facilitating data sharing between business actors and public authorities in cases of exceptional need as well as cloud switching to avoid lock-in effects and open up the market. All these elements are accompanied by efforts to foster a robust data ecosystem that underpins the EU's digital transformation. The EU Commission expects the Data Act to boost the data economy, leading to significant growth in gross domestic product.

To achieve this, the Data Act brings with it a bundle of new rights and obligations for companies, private individuals, and the public sector. It aims to nurture new business models and new forms of cooperation within its regulatory framework. Businesses, public sector bodies, and other data actors are called upon to align with the far-reaching requirements and possibilities introduced by this new EU regulation.

But will the Data Act truly fulfil its ambitious objectives? Will it actually encourage broader data access and use by individuals and businesses, foster innovation, boost the data economy and lay the foundation for a competitive and fairer EU data economy? Critical voices have emerged ever since the first drafts were made public and persist even after the adoption of the final legal text. Some concerns are valid: For example, the relationship between the Data Act and existing data protection rules – including the General Data Protection Regulation – remains only partially resolved, with both frameworks often applying in parallel. The protection of trade secrets is also inadequately regulated and could thus have the opposite effect to the goal of promoting innovation. Those subject to this law must therefore rise to the challenge of adapting to a constantly evolving and sometimes overlapping legal system and rethinking risks for their product and business model development.

We are nevertheless convinced that the Data Act can make a significant contribution to improved, fair, and competitive data usage as well as opening up cloud services and boosting interoperability. A decisive factor for success will be a sound understanding of the rights and obligations laid down in the Act. Only those who

are aware of which rights they enjoy, the requirements the Data Act places on new business models, and what duties now apply to all market participants, will be able to confidently implement and benefit from these new instruments. Only those who are prepared for the new set of obligations can avoid administrative proceedings with possible fines and civil proceedings, thereby protecting their company from damage.

We have thus approached the project of an introductory volume to the Data Act with considerable commitment and pleasure. The present explanations are the result of many hours of analysis, discussion, and practical experience with data-driven projects and legal advice for data-driven companies. We are especially pleased to publish this work in English, enabling our reflections on the practical application of the Data Act to be received and discussed across the EU. We are convinced that the potential of the Data Act can only be realised if there is a broad, fundamental understanding of this new framework, and if we manage to discuss the critical points broadly and thus optimise them in future amendments to the regulation. It is our hope that this introductory volume provides an accessible starting point and valuable compass.

Against this backdrop, we were delighted to realise this project with the outstanding editorial team at Nomos Verlag, especially Dr. Marco Ganzhorn and Mr. Christoph Krampe. This Practitioner's Guide is part of a highly relevant, comprehensive and valued series of volumes, handbooks and commentaries on the various new legal acts arising from the EU Digital Strategy, published in partnership with Verlag C.H.Beck and Hart Publishing.

You now hold in your hands a concise introduction to the Data Act, available shortly after its key obligations have become applicable in all EU Member States on 12.9.2025, and even before the remaining obligations come into full effect on 12.9.2026. We hope this guide forms a solid foundation for establishing a first understanding of and access to this new act. This Practitioner's Guide not only addresses the articles of the Data Act itself, but also examines the surrounding challenges that may arise in the application of its instruments – including legal protection against decisions based on the Data Act. Instead of a detailed article-by-article commentary, we present its subject areas in context and in terms of their practical significance.

This volume seeks to provide guidance not only to companies seeking to unlock the Data Act for new business models, but also to companies, public authorities and other stakeholders wishing to review or develop their own data strategies in light of new competences or obligations under the Act. The same applies to all those called to shape and supervise the European data landscape going forward. Where implementation in national law still bears relevance – despite the direct applicability of EU regulations – we use Germany as an illustrative example.

We wish to thank the publishers for their unwavering support, in particular Dr. Marco Ganzhorn and Mr. Christoph Krampe. Their dedication made it possible to complete this introductory work with such quality and at an impressive pace.

Our gratitude also goes to those who assisted in organising and, above all, proofreading this volume, and without whose efforts the manuscript could not have advanced so swiftly. Special thanks go to our assistants Katharina Oschwald and Natascha Knechtel, as well as our research associates Pauline Brinke, Michèle Nickel and Benjamin Fischbach, for their precise and patient support!

We look forward to supplementing this Practitioner's Guide in due course with emerging developments – including the full realisation of the EU Data Strategy. While the Data Act centres on commercial and user-generated data, its interplay with other frameworks will be an exciting field of further analysis. Until then, it is our hope that this work provides helpful guidance and inspiration for all those affected by, or entitled under, the Data Act's instruments. We welcome comments, discussions and pointers to sections warranting improvement – please feel free to contact us.

Cologne, January 2026

Kristina Schreiber *Patrick Pommerening* *Philipp Schoel*

Contents

Preface V
Authors XV
Abbreviations XVII
General bibliography XXIII

CHAPTER 1
THE EU DATA AND DIGITAL STRATEGY

A. EU Data Strategy 1
B. EU Digital Strategy 4
C. The EU's Omnibus Initiative with the Digital Package on Simplification 7

CHAPTER 2
OVERVIEW AND SCOPE OF THE DATA ACT

A. Goals 9
B. History of the Regulation 10
C. Scope of application 11
I. Subject matter 11
II. Data covered 12
III. Addressees 12
IV. Marketplace principle 13
D. Relationship to other regulations and contract design 13
I. Data protection and trade secret protection 14
II. Freedom of contract 15
E. Entry into force and implementation period 15
I. Validity from September 2025 16
II. Product design obligations: applicable only from September 2026 16
F. Symmetrical vs. asymmetrical regulation of the data economy 17

CHAPTER 3
DATA ACCESS AND MAKING DATA AVAILABLE

A. Regulation system 21
I. Structure 21
II. Exemptions for SMEs 22
B. Actors 23
C. Subject matter of the data access 26
I. Connected products 26
II. Related services 27
III. Usage data and no content data 29
IV. Virtual assistants 30

D. Data access rights 31
I. Factual data access claim: access by design 31
1. Obligated party 31
2. Material organisation 31
3. Generated data 32
4. User account 33
5. Legal consequences of non-compliance 33
6. Deviating agreements 34
II. Making data available by the data holder 35
III. Sharing data with third-party data recipients 36
IV. Duty to provide information 37
V. Data protection law and data access 39
VI. Restrictions on data access outside of data protection law 41
1. Security requirements 41
2. Restriction of competition pursuant to Art. 4(10), Art. 6(2)(e) DA 41
3. Relationship to trade secrets law 43
a) Data as a trade secret 43
b) Protection mechanisms in case of a data access request by the user 44
aa) Appropriate confidentiality measures as a prerequisite for access 44
bb) Withholding of data sharing in the event of a lack of secrecy 46
cc) Refusal of access in the event of serious economic damage .. 47
c) Protection mechanisms in case of a data access request in favour of third parties pursuant to Art. 5 DA 48
d) Technical protective measures in accordance with Art. 11(1) DA 49
e) Requirements for demonstrating the existence of a trade secret 50
4. No restrictions from database law 50
5. Restrictions arising from competition law 52
VII. Limitations on the use and disclosure of data by the data holder 52
1. Limited data use 53
2. Prohibition of data sharing 53
E. Making data available 53
I. Requirements for making data available 54
1. Area of application 55
a) Business-to-business relations 55
b) Obligation to make data available 56
c) Time of application 56
2. Making data available on FRAND terms 56
a) Fair, reasonable and not discriminatory 57
b) Procedure for determining FRAND 58
3. Transparency requirement 59
4. Ineffectiveness of unfair contract terms 60
5. Prohibition of discrimination 61
6. Protection of the user's data sovereignty 61
II. Compensation for making data available 62

III. Dispute settlement 63
1. Area of application 63
2. Requirements for certification 64
3. Costs 65
4. Relationship with courts and other bodies 65
5. Effect of the decision 65

CHAPTER 4
UNFAIR CONTRACTUAL TERMS

A. Introduction 66
B. Scope of application 66
I. Personal scope 67
II. Material scope 67
III. Temporal scope of application 68
C. Relationship to the Unfair Contract Terms Directive 68
D. Unilateral imposition 69
E. Unfair terms control 70
I. Black clauses (Art. 13(4) DA) 70
II. Grey clauses (Art. 13(5) DA) 70
III. General clause (Art. 13(3) DA) 72
IV. Legal consequences 73

CHAPTER 5
SWITCHING BETWEEN DATA PROCESSING SERVICES:
CLOUD SWITCHING

A. Overview 74
B. Addressees and services covered 76
I. Data processing services 76
1. Cloud computing services 77
2. Hosting in the narrower sense 79
3. Edge computing services 79
II. Privileging of on-premise services 80
III. Original and acquiring providers 80
IV. No privileges for SMEs 80
V. Beneficiary customers 81
VI. Application exceptions 81
1. Customised data processing services 81
2. Data processing services for testing and evaluation purposes 82
VII. Switching to similar services, ICT infrastructure or simultaneous use of several providers 82
C. Requirements for data processing services 83
I. Technical aspects of the change 83
1. Infrastructure provider – IaaS 83
2. Providers of data processing services in other respects 84
3. Limitations 84

II. Switching charges 85
III. Duty of loyalty 85
IV. Contract and information 85
1. Publication obligation on the website 86
2. Customer information 86
3. Contract drafting and standard contractual clauses 86

CHAPTER 6
INTEROPERABILITY AND SMART CONTRACTS

A. Overview 90
B. Interoperability for data spaces and data sharing 91
C. Interoperability of data processing services 91
D. Interoperability for smart contracts 92

CHAPTER 7
EXCEPTIONAL NEED TO USE DATA

A. Introduction 94
B. Legal requirements 95
I. Entitled entities 96
1. Public sector bodies 96
2. Union bodies 96
3. Exclusion of application 96
II. Obligated parties 97
III. Legal requirements 97
1. Data request 97
a) Formal requirements 98
b) Material requirements 100
2. Exceptional needs 100
a) Responding to a public emergency 100
b) Fulfilment of specific tasks in the public interest 101
IV. Fulfilment and rejection of data requests 102
V. Relationship to other obligations to provide data 104
C. Scope of use 105
I. No further use under DGA and Open Data Directive 105
II. Obligations of the authorised bodies 105
III. Forwarding of the data obtained to other public bodies 106
D. Compensation for making the data available 108
E. Assistance and cross-border cooperation 109
F. Legal protection 109

CHAPTER 8
SUPERVISION AND ENFORCEMENT

A. Supervisory authorities 112
I. National design options 112

II. Independence 114
III. Data coordinator 115
IV. Responsibility and appointment of representatives 115
B. Penalties 116
C. Right of complaint and legal remedies 117
I. Right of complaint 117
II. Protective letter 118
III. Legal remedies 118
D. Civil court enforcement 120

CHAPTER 9
INTERNATIONAL DATA TRANSFER IN ACCORDANCE WITH THE DATA ACT

A. Introduction 121
B. Norm addressees 121
C. Third country transfer 122
I. International transfer 123
II. State access 124
III. Permissible compliance with official and court decisions 124
D. Protective measures 127

CHAPTER 10
THE EUROPEAN DATA INNOVATION BOARD

A. Introduction 128
B. Staffing 129
I. Task of the Commission 129
II. Members of the EDIB 130
III. Organisation 131
C. Tasks 132
I. Development of standardised practices 132
II. Development of standardised guidelines 133
III. Standardisation activities 133
1. Use and development of cross-sector standards 134
2. Data economy in the internal market 134
IV. Guidelines on 'Common European Data Spaces' 135
V. Facilitating cooperation 136
VI. Other tasks 137

Annex: Data Act 139

Index 231

Authors

Dr. Kristina Schreiber

Dr. Kristina Schreiber is an attorney and partner at Loschelder law firm. She is a specialised lawyer for administrative law and CIPP/E. She specialises in advising on regulatory issues, data protection, data usage, cybersecurity and artificial intelligence. With extensive experience advising corporations and public institutions, she focuses on the legal challenges arising from digital transformation and data-driven business models. Dr. Schreiber regularly publishes and speaks on topics relating to regulatory compliance, privacy and digital law. She is a lecturer at the University of Cologne and the FernUniversität in Hagen.

Dr. Patrick Pommerening

Dr. Patrick Pommerening is an attorney and partner at Loschelder law firm. He is a specialist in and advises on all issues relating to intellectual property law. His work focuses on all legal issues related to the acquisition, transfer and licensing of intellectual property, software and data, as well as the protection of trade secrets and know-how. Dr. Pommerening has many years of experience in drafting and negotiating IP contracts of all kinds, in particular license agreements, research and development agreements as well as software and IT contracts.

Philipp Schoel

Philipp Schoel was a lawyer at Loschelder law firm and specialised in data protection and IT law. He advised on the new European digital legislation and is co-author of the Practitioner's Guide on the Data Governance Act. His legal practice focused on data protection-compliant business models and the related contract drafting.

CHAPTER 1
THE EU DATA AND DIGITAL STRATEGY

Bibliography: Schmitz, 'Digitale-Gesetze-Strategie – Agilität oder „Act"ionismus?', ZD 2022, 189; Schreiber/Brinke, Datenschutz im EU-Gesundheitsdatenraum, PinG 2024, 251; Schreiber/Pommerening/Schoel, New Data Governance Act, A Practitioner's Guide, 2023.

A. EU Data Strategy 4
B. EU Digital Strategy 15
C. The EU's Omnibus Initiative with the Digital Package on Simplification 26

The **EU Digital Strategy** aims to position the European Union at the forefront of the development of the digital economy in a unified single market without borders by fostering a competitive, secure, and inclusive digital surrounding. It focuses on building a **digital single market** that benefits citizens, businesses, and governments, promoting innovation, and ensuring that digital technologies contribute to a sustainable and fair society. The public and private sectors are both involved. The EU expects the digital offensive to lead to a noticeable increase in the gross domestic products of the EU Member States and more prosperity for the society. **1**

Complementing this, the **EU Data Strategy** as part of the EU Digital Strategy seeks to create a single European data space where data can flow freely and be accessed and utilised efficiently, securely and interoperably. This strategy envisions a data-driven economy that leverages the vast amounts of data generated within the EU to drive growth, innovation, and societal progress, as well as more trust in data intermediaries and altruistic data organisations.[1] **2**

With the Data Governance Act (DGA) and the Data Act (DA), the EU has adopted two key measures on the way to an EU-wide data economy: **3**

- The **Data Governance Act** was published as Regulation (EU) 2022/868 in the Official Journal of the EU on 3.6.2022 (OJ 2022 L 152, 1). It is officially referred to as the 'Regulation on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)'.
- The **Data Act**, also an EU Regulation, whose official title is 'Regulation on harmonised rules for fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)', was published as Regulation (EU) 2023/2854 in the Official Journal of the EU (OJ L, 2023/2854) on 22.12.2023.

Together, these two legal acts form the backbone of the EU Data Strategy. In November 2025, a simplification of the Data Governance Act and Data Act is planned, initiated with the draft of a Digital Package on Simplification by the EU Commission (→ mn. 26 et seqq.).

A. EU Data Strategy

As components of the EU Commission's **Data Strategy**, the DA and DGA are embedded in Brussels' comprehensive Digital Strategy. In its Communication of **4**

[1] Details cf. Schreiber/Pommerening/Schoel, New Data Governance Act. A Practitioner's Guide, Baden-Baden 2023, Ch. 3, Ch. 4.

19.2.2020 on a European Data Strategy,[2] the Commission outlines policies and investments to help build an efficient, innovative data economy, in line with European values, fundamental rights and rules.[3] According to the Commission, it is important to harness the potential of the growing amount of existing data for social and economic well-being by improving **access to data** and **promoting responsible data use**.[4]

5 The Commission's vision is a **single European Data Space**, i.e. an internal market for data where both personal and non-personal data is securely handled, where companies can easily access the data they need and (re)use it in compliance with applicable laws (across industries) – regardless of where it is stored in the EU.[5] In addition, the EU aims to ensure free and secure data flows with **third countries**, meaning that the European data space should be accessible to data from all over the world.[6]

6 The DGA and the DA aim to create suitable framework conditions for a **data-agile European economy**.[7] Both Regulations are cross-sectoral measures for data access and use.[8]

7 Based on identified problematic areas in the European data economy, the policy measures and financial support planned in the Data Strategy are divided into **four pillars**:

8 1. The first objective is to establish a cross-sectoral governance framework for **data access and data use** that avoids inconsistent approaches in the various sectors and Member States in the internal market.[9] The DA, with its data access requirements, and the DGA are the main instruments for achieving this objective. As horizontal measures, the DA and DGA address various players in the data economy across sectors.[10] The relationships between the stakeholders, in particular their rights and obligations, are to be standardised across the EU in order to promote the shared use of data, distribute the added value of data more fairly and increase the overall availability of data.[11]

9 A further component is the Implementing Regulation (EU) 2023/138 establishing certain high-value datasets (HVD) and the modalities of their publication and re-use, which supplements the Open Data Directive (EU) 2019/1024. The high-value datasets classified as such by the EU Commission and the Committee on Open Data and the Re-Use of Public Sector Information (see Art. 16(1) Open Data Directive) and included in the list must fulfil the conditions of Art. 14(1) subpara. 2 Open Data Directive after adoption of the implementing

[2] 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' (19.2.2020), COM(2020) 66 final.
[3] COM(2020) 66 final, 1 et seq.
[4] COM(2020) 66 final, 4 et seq.
[5] COM(2020) 66 final, 4 et seq.; rec. 2 sent. 1 DGA.
[6] COM(2020) 66 final, 4 et seq.; rec. 2 sent. 1 DGA.
[7] COM(2020) 66 final, 12.
[8] COM(2020) 66 final, 12.
[9] COM(2020) 66 final, 12.
[10] COM(2020) 66 final, 12.
[11] COM(2020) 66 final, 13 et seq.; European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' (23.2.2022), COM(2022) 68 final, 2 et seq.

act. They must therefore be available free of charge, in machine-readable formats, via APIs and, where relevant, as a bulk download. With a view to the work in the committee, the German Federal Ministry for Economic Affairs and Climate Action had a study prepared on high-quality datasets in Germany, which was published on 10.2.2021.[12]

2. The second pillar of the Data Strategy aims to support **innovative, data-based business models** (especially financially) and to create the necessary infrastructural conditions for the vision of a single European Data Space.[13] After all, realising the potential of the European data economy requires data, cloud infrastructures and corresponding services that enable secure, sustainable, interoperable and scalable data storage and processing.[14] 10

A first practical example of such a data space is the **European Health Data Space (EHDS)**: With its Regulation on the European Health Data Space (Regulation (EU) 2025/327 – 'EHDS Regulation'), the EU legislator has taken the first step towards creating a sector-specific common data space. The EHDS Regulation entered into force on 26.3.2025 and will be applicable from 26.3.2027 onwards. The EHDS is intended to establish a kind of platform – a decentralised data space – on and in which natural persons can post their health data and control further processing (primary data use). The EHDS Regulation is in its structure and idea based on the Data Governance Act.[15] 11

The **EHDS Regulation** is intended to create provisions for common standards and procedures, infrastructures and a governance framework within which health data can be used for primary and secondary purposes.[16] The Regulation is based on the right of patients to access their electronic health data in a secure environment, where they can make sovereign decisions about making this data available for further processing. This will be based on a central platform for health services – **MyHealth@EU** – set up by the Commission, and a canon of obligations for systems for electronic patient records and so-called wellness applications, which, among other things, prescribes certain technical requirements and compliance with common specifications (primary use). Research and innovation stakeholders and political decision-makers should then be able to utilise this data in a trustworthy and secure manner (secondary use).[17] This regulation of secondary data use will also be highly relevant in the context of the training data required for AI applications and research. This is particularly true in light of the fact that the EHDS Regulation will also regulate the use of data under data protection law and create a corresponding basis for authorisation. This is a significant difference and advantage compared to the DA and DGA, which merely leave the GDPR 'untouched' and thus do not solve the data protection challenges. 12

[12] See <https://www.bmwk.de/Redaktion/DE/Publikationen/Studien/studie-hochwertige-datensaetze-in-deutschland.html> (last accessed: 7.1.2026).

[13] COM(2020) 66 final, 15 et seqq.

[14] COM(2020) 66 final, 20 et seq.

[15] COM(2022) 197 final, 4 et seq.

[16] Comprehensive overview by Schreiber/Brinke PinG 2024, 251 et seq.; Ruff/Schreiber EuDIR 2025, 318.

[17] Cf. COM(2022) 197 final, 1.

13 3. The Commission also believes that the EU needs more qualified workers, data experts and overall **data literacy** throughout the population.[18] To achieve this, financial resources should be channelled into training and recruiting talent, women should be more involved and companies should receive targeted advice and support in order to develop and efficiently use data-based business models.[19] The Commission also plans to further empower individuals with regard to their data. There are discussions about strengthening the right to data portability under Art. 20 GDPR, giving individuals more control over who can access and use machine-generated data.[20]

14 4. In addition to the above, the European Commission has announced the development of **common European Data Spaces in strategic sectors and areas of public interest**.[21] Data spaces are initially to be established in nine different sectors (manufacturing, 'Green Deal', mobility, health, finance, energy, agriculture, public administration, skills).[22] More detailed descriptions of these sectors and sector-specific measures can be found in the annex to the Data Strategy.[23]

B. EU Digital Strategy

15 The Data Strategy forms part of the EU Commission's broader Digital Strategy. The Digital Strategy is a comprehensive policy document published together with the Data Strategy on 19.2.2020. In its Communication **'Shaping Europe's digital future'**,[24] the EU Commission presented more than 50 specific key measures,[25] which together form the Digital Strategy. With the Digital Strategy, the EU Commission meets the 'twin challenge of green and digital transformation' and announces a 'substantial societal transformation' to achieve a 'better digital future for everyone'.[26] The aim is to shape the digital transformation – based on European values – in a way that benefits everyone, puts people at the centre and creates new opportunities for the economy.[27]

16 The Digital Strategy is based on **three key objectives**:

- First, to develop and deploy trustworthy **technology that works for people**, transforming their daily lives while respecting European values.
- Second, to promote a **fair and competitive economy** in the single market, where all businesses have the opportunity to increase their productivity and global competitiveness by developing, marketing and using digital technologies,

[18] COM(2020) 66 final, 10 et seq.
[19] COM(2020) 66 final, 20 et seq.
[20] COM(2020) 66 final, 20 et seq.
[21] COM(2020) 66 final, 21 et seq.
[22] COM(2020) 66 final, 22 et seq.
[23] COM(2020) 66 final, 26 et seqq.
[24] 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' (19.2.2020), COM(2020) 67 final.
[25] Critically and instructively Schmitz ZD 2022, 189.
[26] COM(2020) 67 final, 1.
[27] COM(2020) 67 final, 1 et seq.; European Commission, see <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade> (last accessed: 7.1.2026).

products and services, and where consumers can be confident that their rights are respected.
– And third, digital technologies should contribute to an **open, democratic and sustainable society**.[28]

The Commission describes how it intends to shape Europe's digital future and achieve its goals in three sections, which are subordinated to the key objectives. The respective **key measures** are listed at the end of each section and, in some cases, provided with a timeframe for implementation. As one of these key measures, the European Data Strategy falls under the second aspect – promoting a fair and competitive economy. 17

Key aspects of the agenda include accelerating the expansion of **digital infrastructures** and networks, creating the necessary **trust in the security** of digital applications and products, both with regard to cyber threats and the technology itself (especially artificial intelligence-based technology), and investing in digital **skills for all Europeans**. In addition, **fair access** to data should be ensured, data sharing should be encouraged and the market power of large digital corporations and companies should be limited.[29] 18

Core elements of the Digital Strategy have now been implemented and came into force. Following the GDPR in 2018, other Regulations and Directives that must be observed for digital offerings and the handling of (personal and non-personal) data have been in force for several years now, in particular the Platform-to-Business Regulation (Regulation (EU) 2019/1150), the Regulation on the Free Movement of Data (Regulation (EU) 2018/1807) and finally the Directive on Digital Content and Services (Directive (EU) 2019/770) as well as the Directive on certain contractual aspects of the sale of goods (Directive (EU) 2019/771 – Sales of Goods Directive), which also covers goods with digital elements. 19

In the lead-up to the 2024 European Parliament elections, additional legislative components of the Digital Strategy were adopted and entered into force. In addition to the Data Strategy, the most important regulatory areas of the more recent legislative procedures relate to the regulation of digital gatekeepers, information security and the regulation of artificial intelligence: 20

– **Digital gatekeepers**: Two central measures of the Digital Strategy, the Digital Services Act (Regulation (EU) 2022/2065) and the Digital Markets Act (Regulation (EU) 2022/1925), particularly affect online platforms and digital players with market power. The Digital Services Act (DSA) introduces a revised legal framework that defines the responsibilities and obligations of intermediary services such as online platforms. The Digital Markets Act (DMA) complements competition law and limits the power of large platforms with significant network effects that act as gatekeepers. The EU Commission has designated several gatekeepers, including Alphabet (Google), Apple, Amazon, ByteDance, Meta and Microsoft.[30] Both Regulations entered into force in November 2022. 21

[28] COM(2020) 67 final, 2 et seq.
[29] See the overview at: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade> (last accessed: 7.1.2026).
[30] See <https://digital-markets-act.ec.europa.eu/gatekeepers_en> (last accessed: 7.1.2026).

22 – **Artificial intelligence (AI)**: The EU aims to establish a legal framework for trustworthy AI that enhances public confidence in AI-based solutions while encouraging innovation and investment.[31] In April 2021, the EU Commission presented its AI package, including a proposal for a Regulation with harmonised rules for artificial intelligence.[32] The original objective of taking an early pioneering role in the risk regulation of AI applications through rapid adoption was only partially achieved. After intensive negotiations, a political agreement on the AI Regulation was reached in spring 2024. The AI Act was published in the Official Journal of the European Union on 12.7.2024 (Regulation (EU) 2024/1689). The AI Act introduces a risk-based approach that prohibits the use of AI for forbidden practices with an unacceptable risk and intensively regulates AI systems with a high risk. Transparency obligations are imposed on specific AI models, systems and outputs (esp. deepfakes). Finally, there is, among other things, an obligation to develop AI literacy, special regulations for GPAI models, and various requirements for market surveillance and enforcement.

23 – **Cybersecurity**: Especially for digital solutions, cybersecurity is a key factor for confidentiality, availability and integrity. The experience of numerous cyberattacks in recent months and years has emphasised the importance of this issue to the general public. In order to increase the confidence of people and companies in the security of their applications and products, the Digital Strategy also provides for a wide range of measures to strengthen resilience to cyber threats.[33] At its heart is the EU Cybersecurity Strategy for the Digital Decade,[34] which sets out the direction of EU cybersecurity policy. In implementing the Security Strategy, the NIS2 Directive (EU) 2022/2555 and the CER Directive (EU) 2022/2554 on critical infrastructure was announced for the turn of 2023. The Cyber Resilience Act, a Regulation that addresses the security of digital products (Regulation 2024/2847), was published in November 2024. Under the Cyber Resilience Act, security updates will become a clear obligation for the life cycle or five years for digital products, whichever is longer.

24 The various legal acts of the Digital Strategy affect all digital services and products, as well as the handling of data. They have different but overlapping objectives. A major and justified **criticism** of the new legal acts is that they are not harmonised in detail: Most of them provide that other legal acts, in particular the GDPR, are not affected. This leaves considerable legal uncertainty, which in the worst-case scenario could have a negative impact on innovation and Europe as a place to do business. This issue is addressed by the Digital Package on Simplification described in → mn. 26 et seqq.

25 This can be clearly seen, for example, in the **definition of data**: While the GDPR defines data as 'information' about a natural person (digital, analogue in any form; Art. 4(1) no. 1 GDPR), DA (Art. 2 no. 1), DGA (Art. 2 no. 1) and DMA (Art. 2 no. 24) describe data as a digital representation of acts, facts or information, including the form of sound, visual or audiovisual recordings. However, these laws refer to

[31] COM(2020) 67 final, 5.
[32] AI Regulation proposal: COM(2021) 206 final.
[33] COM(2020) 67 final, 5.
[34] European Commission, 'Joint communication to the European Parliament and the Council: The EU's cybersecurity strategy for the digital decade' (16.12.2020), JOIN(2020) 18 final.

Art. 4 no. 1 GDPR for the definition of personal data. This leads to an unclear understanding of what constitutes 'data', especially as the GDPR is supposed to prevail in case of a conflict. The differences in the definition of processing are less serious, but the GDPR is also open to analogue forms; the definition in the DA refers only to digital data.

C. The EU's Omnibus Initiative with the Digital Package on Simplification

In November 2025, the European Commission published a **proposal** for a regulation aimed at revising and simplifying digital legislation: The Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024.[35] It is abbreviated as 'Digital Omnibus on digital acquis'. The planned legal act will also affect the Data Strategy, Data Governance Act, and Data Act. **26**

This proposal is part of the European Union's **'Omnibus Initiative'**, which arises from the recognition that the increasing complexity of digital legislation poses significant challenges to legal certainty and regulatory coherence. The rationale behind the Omnibus approach is to streamline and modernise existing frameworks by introducing coordinated amendments to multiple interconnected legal instruments simultaneously. This strategy aligns directly with the objectives of the Draghi Programme, which prioritises legislative simplification as a means to foster a more dynamic, efficient, and innovation-friendly EU internal market. **27**

The choice to focus on **simplification** in the digital sector is particularly pertinent. Digital regulation in the EU has expanded rapidly over the past decade, often not fully coordinated and harmonised with each other in the individual digital acts. The rapid and overlapping drafting of various legal acts led to overlaps, contradictory definitions, and fragmented legislative amendments, which shall be resolved by the Omnibus legislation. **28**

With the upcoming 'Digital Package on Simplification', the European Commission intends to **simplify** the digital regulation specifically targeting adjustments across the main digital legislative acts. The proposed regulation touches several legal acts, e.g. the GDPR, but also the Data Act. Regarding the Data Act, this package will refine certain definitions (for instance, those relating to data intermediaries and gatekeepers), standardise enforcement provisions and streamline reporting obligations. The initiative also responds to feedback from national authorities and businesses calling for greater coherence and predictability in the EU's digital acquis. The Data Governance Act is to be repealed and incorporated into the Data Act in relevant parts. Those amendments to the Data Act are summarised in Art. 1 of the proposed Regulation.[36] **29**

First, the proposal will consolidate and streamline several rules in the Data Act as the future core Regulation for the data economy: The revised Data Act **30**

[35] COM(2025) 837 final.
[36] COM(2025) 837 final, 20.

shall absorb and replace the Free Flow of Non-Personal Data Regulation (EU) 2018/1807, the Data Governance Act (Regulation (EU) 2022/868), and the Open Data Directive (EU) 2019/1024, consolidating previously fragmented regimes into a **single legal framework**.[37]

31 Second, the Data Act itself is to be further developed in some details. Art. 4(8) of the proposed revised Data Act shall include a right for data holders to refuse to disclose **trade secrets** if there is a high risk of unlawful access, particularly to third-country recipients in jurisdictions with weak or non-equivalent protections. This ground builds on objective factors such as confidentiality levels and enforceability of protection and requires timely written notification to users and authorities.[38] However, the conditions for such a refusal will remain strict, and the possibilities for resorting to it are limited to a few cases. The public sector data sharing (business-to-government, B2G) shall be narrowed to cover only **'public emergencies'** (as newly defined in Art. 2(29)).[39] Further some more **exemptions for SMEs** are planned. Art. 36 dealing with smart contracts shall be deleted due to market immaturity and risk of legal uncertainty.

32 From the Free Flow of Non-Personal Data Regulation especially the prohibition of any non-personal data localisation requirements is reaffirmed and transferred to the Data Act, with a reporting and notification obligation to the Commission by Member States. A **'Single Information Point'** shall provide a searchable register of data assets and simplified information channels (especially for SMEs, SMCs, researchers) to facilitate transparency and re-use across the EU.

33 Although it is not yet clear what form this proposal will take as it goes through the legislative procedure, this Omnibus package will in any case play a decisive role in shaping the framework of future conditions for digital players in the EU. The approach reflects a general shift towards agile regulatory governance and continuous legal harmonisation.

[37] COM(2025) 837 final, 5.
[38] Art. 1(3) COM(2025) 837 final, 24.
[39] COM(2025) 837 final, 35 et seq.

CHAPTER 2
OVERVIEW AND SCOPE OF THE DATA ACT

Bibliography: Bomhard, 'Der Anwendungsbereich des Data Act', MMR 2024, 71; Hennemann/Steinrötter, 'Der Data Act. Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen', NJW 2024, 1; Kumkar, 'Zu den Vorschlägen der EU-Kommission für eine Europäische Datenstrategie', in Baumgärtel/Kiparski (eds), DGRI Jahrbuch 2021/2022, Cologne 2023, p. 51; Pauly/Wichert/Baumann, 'Schutz von Geschäftsgeheimnissen nach dem Data Act', MMR 2024, 211; Steinrötter, 'Verhältnis von Data Act und DS-GVO', GRUR 2023, 216; Wiebe, 'Der Data Act – Innovation oder Illusion?', GRUR 2023, 1569.

A. Goals 1
B. History of the Regulation 7
C. Scope of application 8
I. Subject matter 9
II. Data covered 11
III. Addressees 13
IV. Marketplace principle 14
D. Relationship to other regulations and contract design 16
I. Data protection and trade secret protection 19
II. Freedom of contract 22
E. Entry into force and implementation period 24
I. Validity from September 2025 25
II. Product design obligations: applicable only from September 2026 27
F. Symmetrical vs. asymmetrical regulation of the data economy 36

A. Goals

The purpose of the Data Act, which itself consists of 50 Articles, is to facilitate access, use and disclosure of data generated by the use of connected products or related services (rec. 5 DA). This refers to products that are often referred to as 'smart' – meaning that they are connected to the internet and generate data during their use (the so-called Internet of Things, or IoT for short). The DA goes even further: An internet connection is not necessary. It is sufficient that the products generate data during their use, which can at least be accessed via an interface in the product. **1**

The DA aims to ensure a **fair distribution of the value of data** among stakeholders in the data economy and to promote access to and use of data.[1] It aims to remove barriers to data sharing in order to realise the full potential of data and data-driven innovation.[2] The DA should also enable the public sector to use private data in order to better serve the public interest (business-to-government data sharing).[3] The background to this is that IoT products in particular generate vast amounts of valuable data (rec. 1 DA). However, the EU Commission assumes that 80 % of such industrial data simply remains unused.[4] **2**

[1] COM(2022) 68 final, 2.
[2] COM(2022) 68 final, 1.
[3] Kumkar in Baumgärtel/Kiparski, p. 51 (64 mn. 24).
[4] European Commission, 'Data Law: Commission proposes measures for a fair and innovative data economy' (press release, 23.2.2022) <https://ec.europa.eu/commission/presscorner/detail/de/ip_22_1113> (last accessed: 7.1.2026).

3 As part of the **EU Data Strategy** (→ Ch. 1 mn. 1),[5] the DA aims to create a true single market for data and give Europe a leading role in the global data economy.[6] It is designed to help ensure the innovation and competitiveness of EU businesses, increase the empowerment of individuals with regard to their data and enable businesses and public authorities to better respond to public emergencies and exceptional situations.[7] In addition to fair data use and fair data access, it also focuses on easier switching between data processing services and data interoperability.

4 As a horizontal measure, the DA addresses different **actors in the data economy** across sectors.[8] It aims to standardise the relationships between stakeholders, in particular their rights and obligations, across the EU in order to promote the sharing of data, to distribute the added value from data more fairly and to increase the overall availability of data.[9] The DA is intended to provide a harmonised legal framework setting out the conditions for the use of IoT data (rec. 4 DA).

5 The Commission expects significant **economic growth** as a result of the Data Act. In its impact assessment report, the Commission formulates a significant increase in the GDP of the EU Member States (by 1.98 percentage points by 2028), the expectation of 2.2 million additional jobs and a turnover of almost 200 billion EUR per year by 2028 from data access claims alone.[10]

6 The **main points** of the Regulation are

- the transfer of data between companies and from companies to consumers (access to and supply of data),
- obligations of data holders who are obliged to disclose data under Union law,
- protection against unfair contractual terms in relation to data access and use between companies,
- making data available to public sector bodies and Union institutions, bodies, offices and agencies on grounds of exceptional need,
- switching between data processing services,
- lawfulness of international government access and international transfers of non-personal data,
- interoperability requirements, including for smart contracts.

B. History of the Regulation

7 The Commission introduced the DA through its proposal for a Regulation laying down harmonised rules on fair access to and use of data of 23.2.2022.[11] The DA falls under the first pillar of the EU Data Strategy.[12] As part of the ordinary legislative procedure, the Economic and Social Committee, the European Committee of the

[5] COM(2020) 66 final.
[6] COM(2022) 68 final, 1.
[7] COM(2022) 68 final, 2 et seq.
[8] COM(2020) 66 final, 12.
[9] COM(2020) 66 final, 13 et seq.; COM(2022) 68 final, 2 et seq.
[10] European Commission, 'Commission Staff Working Document: Executive summary of the impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' (23.2.2022), SWD(2022) 35 final, 2.
[11] COM(2022) 68 final.
[12] COM(2020) 66 final.

Index

Bold numbers refer to chapters, normal ones to margin numbers.

Access
– fair and non-discriminatory **1** 18
– international **9** 9

Access by design
– deviating agreements **3** 60
– generated data **3** 52
– material defect **3** 59
– non-compliance, legal consequences **3** 55 et seqq.
– obliged party **3** 47
– prerequisites **3** 46
– product design obligation **3** 3
– product design requirements **3** 48 et seqq.
– user account **3** 54

Access procedure **10** 39

Acquiring provider **5** 34 et seqq.

Action for failure to act **8** 39

Addressees **2** 13

Administrative act
– data request **7** 14
– legal remedy **8** 35

AI Regulation **1** 22

Application and enforcement **3** 58

Area of application **2** 8 et seqq.

Artificial intelligence, Digital Strategy **1** 22

Authority, responsible, EDIB **10** 10, 41

Automotive sector **2** 38

Big data analysis **3** 99

Black clause **4** 14 et seqq.

Burden of proof rule, fairness test **4** 12

Business data **10** 28

Business model, Data Strategy **1** 10

Business representative **10** 40

Business-to-Government (B2G) **7** 1

Cancellation, cloud switching **5** 51

Charges, data processing service **6** 10

Charter of Fundamental Rights, related service **3** 36

Civil court enforcement **8** 41 et seqq.
– action for performance **8** 42
– temporary injunction **8** 43

CLOUD Act **9** 20

Cloud computing service
– ENISA **5** 22
– NIST **5** 20
– term **5** 19 et seqq.

Cloud switching **5** 1 et seqq., **8** 41
– addressees **5** 9 et seqq., 34
– cancellation **5** 51
– charges **5** 65
– compatibility **5** 60
– competition promotion **5** 2
– constellations **5** 3
– contract **5** 69 et seqq.
– contract, minimum content **5** 77
– contract design **5** 76
– customer information **5** 72 et seqq.
– destination provider **5** 34 et seqq.
– duty of loyalty **5** 68
– duty to inform **5** 69
– formal requirements **5** 76
– functional equivalence **5** 57
– IaaS **5** 54 et seqq.
– infrastructure provider **5** 54 et seqq.
– lock-in effect **5** 5
– MCTs **5** 82
– online register **5** 75
– open interface **5** 59
– SCCs **5** 8, 76 et seqq., 82
– small and micro enterprise **5** 37 et seq.
– source provider **5** 34 et seqq.
– switch **5** 51
– switching charges **5** 64 et seqq.
– technical aspects **5** 53 et seqq.
– termination **5** 80
– transparency obligation **5** 70 et seq.

Companies, business-to-business relations **3** 137 et seqq.
Compatibility, cloud switching **5** 60
Compensation for making data available **3** 160, **7** 60 et seqq.
– amount **3** 163
Competitive product, non-competition clause **3** 92 et seqq.
Competitor, direct **3** 115
Complaint **3** 109, 113, **8** 26 et seqq.
– compensation for making data available **7** 67
– data access **8** 29
– data request **7** 73
– forfeiture **8** 32
– procedure **8** 27
– public sector body **8** 30
– shape **8** 32
Confidentiality, supervisory authority **8** 10
Confidentiality agreement **3** 105
– intended use **3** 106
Confidentiality measure **3** 102
Conflict clause **2** 17
Connected product **3** 3, 25 et seqq.
– smartphone **3** 28
– term **3** 26
– use cases **3** 27
Connecting Europe Facility **10** 33
Consent form, EDIB **10** 47
Consideration making data available, transparency **3** 165
Consumer
– EU consumer protection law **3** 141
– making data available **3** 139
Content data **3** 42
Contract design **2** 22, **8** 41
– duties, commencement **2** 26
Contractual partner, term **3** 20
Contractual term, unfair **3** 156 et seqq., **4** 1 et seqq.
Contractual term control, making data available **3** 135
Cooperation, cross-border
– data request **7** 68 et seqq.
– notification obligation **7** 69
Customer **5** 39 et seqq.
Customer information, cloud switching **5** 72 et seqq.
Customising **5** 43 et seqq.
Cybersecurity **10** 39
– Digital Strategy **1** 23
– EDIB **10** 27

Dark patterns **3** 155
Data
– accessibility, easy **3** 65
– aggregated **3** 125
– anonymisation, costs **7** 64
– as a trade secret **3** 98 et seq.
– categories **2** 11
– covered **2** 11
– further use **7** 48
– preparation **3** 41
– private sector **2** 12, **7** 10
– pseudonymisation, costs **7** 64
– raw data **3** 99
– sensor-generated **3** 123
– sharing **3** 154
– term **1** 25
Data access **3** 1 et seqq., **8** 41
– actors **3** 12 et seqq.
– ad hoc **7** 46
– claims **3** 45 et seqq.
– complaint **8** 29
– duty to inform **3** 75 et seqq.
– making data available by data holder **3** 61 et seqq.
– negotiations **4** 1
– regulation system **3** 2
– relationship to data protection law **3** 82 et seqq.
– request **3** 114
– restriction **3** 89 et seqq.
– sharing data with third parties **3** 68 et seqq.
– subject matter **3** 24 et seqq.
Data access officer **8** 16
Data acquisition **7** 30
Data altruism, EDIB **10** 24

Database **3** 122 et seqq.
– mixed **3** 124
Database maker right, barrier **3** 122
Data coordinator **8** 12 et seq., 26
Data economy **1** 6
– actors **2** 4
– domestic market **10** 29
– EDIB **10** 35 et seqq.
Data exchange **6** 1
Data expertise **1** 18
– Data Strategy **1** 13
Data extraction fee **6** 10
Data Governance Act (DGA) **1** 30
– third country transfer **9** 3
Data holder **3** 137, 140, **7** 10
– controller under data protection law **3** 19
– data use **3** 127
– right of defence **3** 119
– term **3** 16 et seqq.
– use of data **3** 127
Data holdership **3** 127
Data portability **6** 12
Data processing service **5** 10 et seqq.
– administrative expenses **5** 13
– application exceptions **5** 42 et seqq.
– charges **6** 10
– cloud computing service **5** 19 et seqq.
– computing resources, elastic **5** 16
– computing resources, scalable **5** 16
– customer **5** 39 et seqq.
– distributed computing resources **5** 17
– edge computing service **5** 28
– hosting service **5** 27
– interaction **5** 13
– interoperability **6** 8
– more customised **5** 43 et seqq.
– network access **5** 12
– on-premise service **5** 33
– provider **5** 34 et seqq.
– requirements **5** 52 et seqq.
– shared pool **5** 15
– switching **5** 1 et seqq.
– term **5** 10
– test and evaluation purposes **5** 46
Data protection, EDIB **10** 27
Data protection law **3** 82 et seqq.
– applicability **3** 83
– basis for authorisation **3** 84
– conflict case **3** 83
– relationship to the DA **2** 19 et seq.
Data protection supervisory authority **8** 3
– personal data **8** 4
Data provision, EDIB **10** 25
Data quality, fairness test **4** 15
Data recipient **3** 68
– business **3** 140
– term **3** 23
Data relation, fairness test **4** 4, 19
Data request **7** 14 et seqq.
– administrative act **7** 14
– challenge **7** 74
– competent authority **7** 41
– complaint **7** 73
– cooperation, cross-border **7** 68 et seqq.
– data transfer, notification obligation **7** 59
– data transfer for research purposes **7** 56
– data transfer to public authorities **7** 53 et seqq.
– data transfer to third parties **7** 54
– GDPR **7** 76
– informal requirement **7** 15
– information request **7** 19
– legal protection **7** 72 et seqq.
– legal protection, third parties **7** 77
– making data available **7** 32
– model template **7** 21
– modification **7** 35
– personal data **7** 40
– rejection **7** 35, 39
– relationship to other data provision obligations **7** 42 et seqq.
– requirements, formal **7** 17 et seqq.
– requirements, material **7** 20 et seq.
– rescissory action **7** 75

– risks **7** 38
– scope of usage **7** 47 et seqq.
– trade secret, disclosure **7** 34
– trade secret, protection **7** 50
Data room **10** 33
Data sharing **3** 154
– agreement **3** 134, 156
– interoperability **6** 5 et seqq.
– user requirements **3** 71
Data sovereignty, user **3** 159
Data space
– Data Strategy **1** 14
– interoperability **6** 5 et seqq.
Data Strategy **1** 4 et seqq., **2** 3
– business models **1** 10
– data expertise **1** 13
– data space **1** 14
– data usage **1** 8
Data transfer
– data coordinator **8** 12 et seq.
– EDIB **10** 25
– international **9** 8 et seqq.
Data use
– cross-sectoral **10** 32 et seqq.
– data holder **3** 127
– Data Strategy **1** 8
– limited **3** 129
– non-personal data **3** 129, **7** 29
– personal data **3** 129
Destination provider **5** 34 et seqq.
Digital health authority **10** 37
Digital Markets Act (DMA) **1** 21
Digital Omnibus **1** 26 et seqq.
– trade secrets **1** 31
Digital Services Act (DSA) **1** 21
Digital Strategy **1** 15 et seqq.
– Artificial Intelligence **1** 22
– components **1** 19
– cybersecurity **1** 23
– gatekeeper **1** 21
– information security **1** 23
– key measures **1** 17
– objectives **1** 16
Disclosure, prohibition **3** 131
Dispute settlement **3** 109, 113
– making data available **3** 166
– subject matter of the dispute **3** 176
Dispute settlement body
– accessibility **3** 172
– certification **3** 171 et seqq.
– decision, effect **3** 177 et seq.
– determination of fees **3** 175
– efficient decision-making **3** 172
– expertise **3** 172
– impartiality **3** 172
– independence **3** 172
– list **3** 174
– making data available **3** 166, 170
– private organisation **3** 173
Dispute settlement procedure
– legal remedy **3** 178
– making data available **3** 170
Duty of loyalty, cloud switching **5** 68
Duty to inform
– cloud switching **5** 69
– data access **3** 75 et seqq.
– making data available **3** 4
Duty to inform, data access
– authorised person **3** 77
– content details **3** 79
– obliged party **3** 76
– provision **3** 77

Edge computing service **5** 28 et seqq.
– description **5** 29
Edge service **5** 28 et seqq.
Effects **2** 5
Entry into force **2** 24
ePrivacy Directive **2** 17, 19
EU Ecolabel **10** 3
European Central Bank (ECB) **7** 5
European Data Innovation Board (EDIB) **10** 1 et seqq., 25
– application **10** 11
– cast **10** 7
– chair **10** 16
– consent form **10** 47
– consultancy, technical **10** 31
– consultancy function **10** 19
– cooperation **10** 41 et seqq.

– cybersecurity **10** 27
– data altruism **10** 24
– data altruistic organisation **10** 44
– data protection **10** 27
– data switching service **10** 44
– EU Commission **10** 16
– exchange of information **10** 44
– expert **10** 13
– expertise **10** 13, 20
– further use **10** 24, 43
– implementation of EU legislation **10** 20
– implementing act **10** 47
– internal organisation **10** 17
– interoperability **10** 36
– meeting **10** 16
– members **10** 8 et seqq., 12
– members, categories **10** 9
– organisation **10** 15 et seqq.
– public body **10** 43
– recommendations **10** 48
– representatives of the authorities **10** 10, 14, 26, 49
– rules of procedure **10** 15
– shared data room **10** 32, 38
– stakeholders **10** 9, 28
– standardisation **10** 29 et seqq.
– standardised guidelines **10** 27 et seq.
– standardised practices **10** 23 et seqq.
– subgroups **10** 17
– subject areas **10** 22
– support function **10** 19
– tasks **10** 18 et seqq., 22
– transparency register **10** 9
– voting **10** 15

European Data Protection Board (EDPB) **10** 4, 10

European Data Protection Supervisor (EDPS) **10** 10
– penalties **8** 24

European Data Space **1** 5

European Health Data Space (EHDS) **1** 11 et seq., **2** 37, **6** 5, **10** 37

European interoperability framework **10** 33

European Union Agency for Cybersecurity (ENISA) **10** 4, 10

Exceptional need **7** 22 et seqq.
– making data available **7** 1 et seqq.
– obligation to provide evidence **7** 31
– public emergency **7** 24 et seqq.
– requirements **7** 13 et seqq.

Exchange of information **10** 44

Exclusion of application **2** 16

Expert group **10** 2
– formal **10** 7
– register **10** 16

Factual control **3** 119

Fairness control, data sharing agreement **3** 156

Fairness test **4** 1, 13 et seqq.
– B2C relationship **4** 9
– black clause **4** 14 et seqq.
– burden of proof rule **4** 12
– Clause Directive **4** 8
– content control, split **4** 5
– data relation **4** 4, 15, 19
– general clause **4** 20 et seqq.
– general clause, good faith **4** 23
– general term, good commercial practice **4** 22
– grey clause **4** 17 et seqq.
– reduction to preserve validity **4** 24
– scope, material **4** 4 et seqq.
– scope, personal **4** 3
– scope, temporal **4** 7
– unilateral imposition **4** 10 et seqq.

Federal Network Agency **8** 2

Financial equalisation
– for making data available **7** 60 et seqq.
– small and microenterprises **7** 61

FRAND conditions **2** 2
– fair **3** 147
– making data available **3** 134, 136 et seqq., 144 et seqq.
– non-discriminatory **3** 147
– patent law **3** 149 et seqq.
– procedure **3** 149 et seqq.
– reasonable **3** 147

Freedom from instructions, supervisory authority **8** 11
Freedom of contract **2** 22
Free Flow of Data Regulation **1** 30, 32
Fulfilment of statutory tasks **7** 28 et seqq.
Functional equivalence
– cloud switching **5** 57
– IaaS **5** 56
Further use
– EDIB **10** 24, 43
– from data **7** 48
Further users, third country transfer **9** 21

Gatekeeper **3** 70
– Digital Strategy **1** 21
General Data Protection Regulation (GDPR) **2** 17, 19, **7** 76
– demarcation **9** 5
– third country transfer **9** 1
General term, fairness test **4** 20 et seqq.
Generated data **3** 52 et seq.
Goals **2** 1 et seqq.
Goods with digital elements **3** 32
Government organisation **9** 11
Government-to-Government (G2G) **7** 10
Grey clause **4** 17 et seqq.
GTC law **4** 11
Guest access **3** 54

Harmonised rules **2** 9
Head office, competence, supervisory authority **8** 14
Health data **10** 37
History of origin **2** 7
Hosting service **5** 19, 27

ICT infrastructure **5** 49
ICT standardisation **10** 33
Implementation deadline **2** 24
Independence, supervisory authority **8** 11 et seqq.
Information security, Digital Strategy **1** 23
Infrastructure **1** 18
Infrastructure-as-a-Service (IaaS)
– cloud switching **5** 54 et seqq.
– functional equivalence **5** 56
Infrastructure provider, cloud switching **5** 54 et seqq.
Innovation, aftermarket **3** 94
Intellectual property **10** 28
International agreement **9** 15
– exceptions **9** 17
International data access, EDIB **10** 25
International transfer **9** 8 et seqq.
Internet of Things product **3** 26
Interoperability **6** 1 et seqq.
– data portability **6** 12
– data processing service **6** 8
– delegated legislation **6** 7, 13
– minimum requirements **6** 4
– smart contracts **6** 14 et seqq.
– specifications and standards **6** 11
– transparency **6** 6

Legal protection **7** 72 et seqq.
– complaint **7** 73
– data request **7** 72 et seqq.
– rescissory action **7** 75
– third party **7** 77
Legal remedy **8** 34 et seqq.
– action for failure to act **8** 39
– administrative act **8** 35
– enforcement action **8** 35
– jurisdiction **8** 40
– multipolar legal relationships **8** 36
– rescissory action **8** 35
– right of action **8** 36
Lock-in effect **10** 39
– cloud switching **5** 5

Making data available **3** 1 et seqq., 132 et seqq., 154
– appropriate consideration **3** 134
– by data holder **3** 61 et seqq.
– compensation **3** 160, **7** 60 et seqq.

– compensation, calculation **7** 63
– compensation, complaint **7** 67
– compensation, transparency **3** 165
– consideration, amount of **3** 152
– consumer **3** 139
– contractual term control **3** 135
– costs **3** 162
– dispute **3** 167
– dispute settlement, out-of-court **3** 166
– dispute settlement body **3** 166, 170
– dispute settlement procedure **3** 170
– duty to inform **3** 4
– entitled body **7** 5
– entitled entity **7** 4 et seqq.
– entitled entity, obligations **7** 49 et seqq.
– exceptional need **7** 1 et seqq.
– FRAND conditions **3** 134, 136 et seqq., 144 et seqq.
– G2G **7** 10
– in situ **7** 33
– investment **3** 162
– legal right of access **3** 63
– obligated party **7** 10 et seqq.
– prohibition of discrimination **3** 158
– real time **3** 64
– regulation system **3** 2
– requirements **3** 64
– sharing **3** 6
– small and microenterprises **7** 11
– time of application **3** 143
– transparency requirement **3** 153 et seqq.
– user requirement **3** 66

Manufacturer **3** 13
– term **3** 15

Marketplace principle **2** 14 et seq.

Material defect, access by design **3** 59

Metadata **3** 53

Mobility Data Space **2** 37

Model Contractual Terms (MCTs) **2** 23, **3** 102, 152, 160 et seq.
– cloud switching **5** 82

Multi-stakeholder platform **10** 33

Mutual legal assistance treaty **9** 15

Network access, location-independent **5** 12

Non-compete clause **7** 50

Non-personal data **3** 85
– use **3** 129

Non-profit research organisation **3** 164

Obligation to make data available **3** 5, 142
– area of application **3** 137
– implementation deadline **2** 25
– start **2** 25

One-stop shop **8** 14

Online register, cloud switching **5** 75

On-premise service **5** 33

Open Data Directive **1** 9, 30

Open interface, cloud switching **5** 59

Original provider **5** 34 et seqq.

Overclaiming **3** 100 et seqq.

Patent law
– compulsory licence **3** 144
– standard-essential patent **3** 144

Penalties
– criteria **8** 20
– EDPS **8** 24
– fine **8** 22, 24
– notification obligation of the Member States **8** 23
– OWiG **8** 20
– recommendations of the EDIB **8** 20

Penalty **8** 19 et seqq.

Personal data **3** 84
– data use **3** 129

Preparation, data **3** 41

Privacy by design **3** 83

Private autonomy **2** 18

Private sector data **2** 12

Product data **3** 37 et seqq.
– term **3** 38

Product design obligation **2** 27 et seqq.
– access by design **3** 3
– relevant date **2** 29 et seqq.
Product version **2** 33
Prohibition of cartels, barrier **3** 126
Prohibition of circumvention **3** 118
Prohibition of discrimination, making data available **3** 158
Prosecution **2** 18
Protection mechanism, data access request **3** 114 et seqq.
Protective letter **8** 33
Protective measure
– appropriateness **9** 26
– legal **9** 24
– organisational **9** 25
– technical **9** 23
– third country transfer **9** 22 et seqq.
Public emergency **7** 24 et seqq.
– determination **7** 27
Public interest **7** 28 et seqq.
Public recognition **7** 60
Public sector body **7** 2, 6
– complaint **8** 30
Purpose **2** 1
Purpose of the contract, determination **3** 115

Raw data, term **3** 40
Reasonable consideration, making data available **3** 134
Refusal of access
– complaint **3** 109, 113
– dispute settlement **3** 109, 113
– duty to substantiate **3** 108
– economic damage **3** 111
– lack of secrecy **3** 107
– notification obligation **3** 108
Regulatory focus **2** 6
Related service **3** 29 et seqq.
– Charter of Fundamental Rights **3** 36
– goods with digital element **3** 32
– term **3** 30
– use cases **3** 31
Related service data **3** 37 et seqq.
– term **3** 39
Relationship to data protection **2** 19 et seq.
Relationship to trade secret protection **2** 21
Relevant market concept, market definition under antitrust law **3** 93
Representative, supervisory authority **8** 15
Representative of the authority **10** 46, 49
Requirement of certainty **3** 116
Rescissory action, data request **7** 75
Research **3** 164
Restriction of competition, competitive product **3** 92 et seqq.
Reverse engineering **3** 94
Right of access to data
– competitor **3** 126
– third party **3** 114
– user-accessible **3** 114
Right of action **8** 36
Right of defence, data holder **3** 119
Right to refuse performance, notification obligation **3** 91

Schrems II **9** 22
Security, requirements **3** 90 et seq., **10** 39
Service data **3** 37 et seqq.
Service type **5** 48
Shared data room **10** 32, 36, 38
Sharing of data **3** 6
Sharing of data with third parties
– limitation **3** 73
– prerequisites **3** 70
Small and medium-sized enterprises (SME) **5** 37 et seq., **7** 11
– making data available, compensation **3** 164
Small and microenterprises
– exceptions **3** 9 et seqq.

– financial compensation **7** 61
– subcontractor **3** 10
Smart contract **3** 117, **6** 1 et seqq.
– interoperability **6** 14 et seqq.
Smartphone **3** 28
Sole source database **3** 123
Source provider **5** 34 et seqq.
Stakeholder **10** 38
– EDIB **10** 9
Standard Contractual Clauses (SCCs) **3** 102
– cloud switching **5** 8, 76 et seqq., 82
Standardisation **10** 29 et seqq.
– cross-sectoral **10** 29 et seqq., 34
– EDIB **10** 29 et seqq.
– interoperability **10** 38
– legal **10** 33
– sector-specific **10** 34
– technical **10** 33
Subcontractor, small and microenterprises **3** 10
Subject matter **2** 9 et seq.
Supervisory authority **8** 2 et seqq.
– competence **8** 14
– confidentiality **8** 10
– consultancy and monitoring **8** 8
– cooperation **8** 9
– data access officer **8** 16
– data protection supervisory authority **8** 3
– freedom from instructions **8** 11
– independence **8** 11 et seqq.
– national **8** 2 et seqq.
– representative **8** 15
– representative, accountability **8** 17
– sectoral **8** 5
– supervision and enforcement **8** 7
– tasks **8** 6
Switching charges, cloud switching **5** 64 et seqq.

Technical and Organisational Measures (TOM) **3** 102
Technical protective measures **3** 117
Termination, cloud switching **5** 80
Third country **9** 6
Third country reference **9** 21
Third country transfer **9** 1 et seqq., **10** 39
– area of application **9** 5
– data processing service **9** 2
– data provision **9** 9
– further users **9** 4
– judicial and official decisions **9** 13 et seqq.
– legal uncertainty **9** 20
– more unlawful **9** 5
– protective measures **9** 22 et seqq.
– US authority **9** 20
Trade secret **3** 96 et seqq., **7** 50
– confidentiality measure **3** 102
– explanation and justification **3** 120 et seq.
– risks **3** 114
– Trade Secrets Directive **3** 121
Trade secret protection, relationship to DA **2** 21, **3** 96 et seqq.
Transparency **6** 6
Transparency obligation, cloud switching **5** 70 et seq.
Transparency register, EDIB **10** 9
Transparency requirements **3** 153 et seqq.
Transport interoperability **6** 12

Unilateral imposition **4** 10 et seqq.
Union body **7** 7 et seq.
Unity of the legal system **2** 35
US authority **9** 20
Use of data
– data holder **3** 127
– further use **7** 48
– research purposes **7** 48
User **3** 13
– data subject under data protection law **3** 22
– term **3** 21
User account **3** 54
User requirements **3** 71

Virtual assistant **3** 43 et seq.