Technical Reports 14

ITeG
Wissenschaftliches Zentrum für Informationstechnik-Gestaltung

Data Governance in Germany – An Introduction

kassel university press

ITeG Technical Reports

Band 14

Herausgegeben vom
Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG)
an der Universität Kassel

Universität Kassel
ITeG Wissenschaftliches Zentrum für
Informationstechnik-Gestaltung
Pfannkuchstraße 1
D-34121 Kassel

Data Governance in Germany –

An Introduction

Authors

Priv.-Doz. Dr. Christian L. Geminn, Mag. iur.

Paul C. Johannes, LL. M.

Johannes K. M. Müller, MLE.

Dr. Maxi Nebel

kassel university press

Impressum:

Project Group Constitutionally Compatible Technology Design (provet)

Chair for Public Law
Prof. Dr. Alexander Roßnagel

Kassel University
Pfannkuchstr. 1
34121 Kassel
Germany

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

ISBN 978-3-7376-1112-1
DOI: https://doi.org/10.17170/kobra-202304127800

https://kup.uni-kassel.de

Umschlagabbildung: shutterstock-Vektorgrafik ID 1995018869

Foreword

This report presents an introduction to and overview of data governance mechanisms, instruments, and approaches with a particular focus on those included in the new "data law" – ushered in by the enactment of the Data Governance Act (Regulation (EU) 2022/868) in May 2022. The goal of the report is to provide a point of reference as well as to highlight the system and roots of data governance in Germany.

The report was written with readers in mind (domestic and abroad) without a strong legal background who nevertheless wish to or need to immerse themselves in the legal aspects of data governance. It aims to serve as an entry point and to enable readers to prepare for the new "data law" and its implications for data governance as well as its interplay with German law.

The report was compiled in the context of the creation of a "Data Governance Playbook" on behalf of the Mozilla Foundation. This report expands on the "Data Governance Playbook" when it comes to providing an overview of the system of data governance in Germany and the particulars of individual mechanisms, instruments, and approaches – it is an extended version of the overview found in the "Playbook". For concrete recommendations for "builders" (as defined by Mozilla Foundation Data Futures Lab: "*individual founders, developers, organizations or companies who design and develop technologies and initiatives that make use of alternative data governance models to unlock the value of data for individuals, communities and society*"; see https://foundation.mozilla.org/de/data-futures-lab/data-for-empowerment/data-futures-lab-glossary/#builders) on which route to go and why when it comes to data governance, please refer to the "Data Governance Playbook", which can be found here:

Is that even legal? A guide for builders experimenting with data governance in Germany, Feb. 15, 2023

https://foundation.mozilla.org/en/research/library/is-that-even-legal/germany/

Readers of the "Playbook" can however find more information and details on data governance instruments not covered by the Playbook in such detail in this report.

Mozilla Foundation has also commissioned and published "Playbooks" for India, Kenya and the United States which can be accessed here:

Landing page:

https://foundation.mozilla.org/en/research/library/is-that-even-legal/builders-guide/

India:

https://foundation.mozilla.org/de/research/library/is-that-even-legal/india/

Kenya:

https://foundation.mozilla.org/de/research/library/is-that-even-legal/kenya/

United States:

https://foundation.mozilla.org/de/research/library/is-that-even-legal/usa/

Kassel, March 2023 The Authors

Contents

A. Legal Framework

Lawful data governance in general refers to the process of handling and managing data in compliance with legal and regulatory requirements. In practice it involves establishing policies and procedures to ensure that data is collected, stored, shared etc. in a way that is consistent with applicable laws and regulations.

Therefore, lawful data governance involves identifying the legal and regulatory requirements that apply to data held by an organisation, as well as establishing processes for managing data to ensure compliance. This is not only essential in order to avoid legal and regulatory penalties, protect one's reputation, and maintain the trust of customers and stakeholders but to also protect society as a whole and the fundamental principles that it is governed by. It requires ongoing monitoring and review to ensure that data management practices remain compliant with changing legal and regulatory requirements.

I. Constitutional Framework

Data governance does not exist in a vacuum. It is subject to numerous prerequisites and requirements which prohibit certain data governance concepts and strengthen or weaken the case for others. The most profound guidelines for data governance are found in the fundamental rights enshrined in the German constitution and at the European level.

1. National Level

The supreme value of the German constitution, the Basic Law (Grundgesetz, GG), is human dignity (Article 1(1) GG). It is the source of all fundamental rights and reflects the intrinsic worth of any human being. While there is no fixed template to determine a violation of human dignity, the German Federal Constitutional Court (Bundesverfassungsgericht) has recognized that a violation can usually be identified in situations in which a human being is objectified.[1]

The second article of the Basic Law then follows with the statement that every person shall have the right to free development of their personality. Together with human dignity, this right is concretized to a general right of personality (Allgemeines Persönlichkeitsrecht). This concretization cannot be found in the text of the Basic Law; it is an unnamed fundamental right that has been recognized since 1954. The general right to personality has since then been used by the Court numerous times as a gateway to the recognition of other unnamed fundamental rights.

One particularly impactful example was the recognition of a right to informational self-determination (informationelle Selbstbestimmung) by the Court in 1983. This recognition has shaped the German approach to data governance significantly. The so-called "census decision" of 1983 contains multiple statements that relate to the processing of personal data on a fundamental level. Regarding the consequences of data processing, the Court stated: "*A person that cannot overlook with adequate certainty which information concerning him are known in certain areas of his social environment, and that cannot somewhat estimate the knowledge of possible communication partners, can be substantially constrained in his freedom to plan or to decide in a self-determinate manner*."[2]

[1] BVerfGE 30, 1 (25).
[2] BVerfGE 65, 1 (43).

The court also stated that due to technological progress (in terms of collecting and combining data) there is no longer any "*inconsequential data*".[3] This means that even seemingly innocuous data must be treated with care, because changes in society or technology might render the data highly or simply more meaningful in the future. All-in-all the right to informational self-determination guarantees the authority of the individual to decide for themself if their personal data is surrendered and used and "*to decide when and under which constraints information pertaining to personal life circumstances are disclosed*".[4] The right thus protects from limitless collection, storage, use and transfer of personal data.

It also prevents the creation of huge repositories of personal data that state entities can access and that provide a comprehensive overview of an individual, as well as linking smaller repositories to the same effect. This is (in addition to the danger of a loss of information control) a consequence of the limitation that the State must not register a human being in the entirety of his or her personality which stems from the much earlier "Micro-census decision" of the Court: *"It would be impossible to reconcile with human dignity if the state were able to claim a right to compulsorily register and catalogue the human being in the whole of his personality, albeit within the anonymity of a statistical ascertainment, and to thus treat him like an object which is accessible to inventory taking in every respect."*[5] In a later decision the Court even stated: *"The requirement that the exercise of their freedoms by the citizens may not be totally recorded and registered is part of the constitutional identity of the Federal Republic of Germany."*[6] As a result, data processing in Germany is usually structured in a decentralized manner with strict regulations for access.

While the fundamental rights enshrined in the Basic Law provide protection against actions of the State (Abwehrfunktion), they also mandate a proactive duty to protect (Schutzpflicht des Staates). This duty means that the State must implement protective measures against violations of fundamental rights by private entities. These protective measures must be sufficient (Untermaßverbot), but the State has significant leeway. In addition to this, the fundamental rights in their totality form an objective normative system of values (objektive Wertordnung) which determines the relationship between citizens. Together with the goal to ensure participation and contribution (Teilhabefunktion), there are thus four basic purposes that fundamental rights serve, and which have an impact on data governance. As a result, the fundamental rights form the framework for data governance both in the public and in the private sector; the fundamental rights have both a vertical and a (limited) horizontal effect.

The processors and controllers of data themselves can rely on the rights according to Articles 12 and 14 GG. Article 12(1)(1) GG contains a right to occupational freedom, which enables Germans to freely choose their occupation or profession, their place of work and their place of training. The right is thus geared towards potentials. Article 14(1) GG guarantees property and the right of inheritance. However, Article 14(2) restricts this by stating that property entails obligations. Its use shall also serve the public good. Property in the sense of Article 14 GG encompasses all rights that relate to existing assets and is broader than property in the sense of German Civil Law. Articles 12 and 14 GG have implications on both the processing of personal data and non-personal data. For data governance, this means that – like any other property – data is meant to serve not only an individual or a company, but also the community as a whole.

In summary, the constitutional framework provides several guiding principles for data governance. A cogent data governance model should

[3] BVerfGE 65, 1 (45).
[4] BVerfGE 65, 1 (42).
[5] BVerfGE 27, 1 (6).
[6] BVerfGE 125, 260 (324).

- enable the individual data subject to assert control over the fact whether or not personal data is processed, and also over the context of said processing (within the limits of other rights and interests);
- avoid the creation of huge data repositories (either sui generis or through the linking of smaller repositories) that enable those with access to these repositories to form an image of the personality of individual data subjects or a close approximation of such an image;
- enable a usage of data that serves the common good and not just individual interests; and
- keep in mind the differences (and similarities) between data usage by the state and by private entities, which can themselves invoke fundamental rights.

2. European Level

At the European level, the Charter of Fundamental Rights of the European Union (CFR) contains a right to protection of personal data. According to Article 8(1) CFR, everyone has the right to the protection of personal data concerning them. This is usually considered in conjunction with Article 7 CFR which guarantees everyone the right to respect for their private and family life, home and communications. In addition, the European Convention on Human Rights (ECHR), which applies to all member states of the Council of Europe, contains in Article 8 ECHR an equivalent to Article 7 CFR which is recognized to also encompass a right to protection of personal data. The equivalents to Articles 12 and 14 GG in the Charter are Articles 16 and 17 CFR. All these rights can be seen as an addition to national fundamental rights. However, the rights found in the CFR can in certain cases even override national fundamental rights.

II. Relevant Laws and Regulations

The following is a collection of the most impactful laws and regulations on sub-constitutional level concerning data governance. Of particular importance for the digital economy and thus data governance are five EU regulations: The Digital Markets Act (DMA), the Digital Services Act (DSA), the Data Governance Act (DGA), the Data Act (DA) and the Artificial Intelligence Act (AIA). These five regulations, which are in different states of the legislative process, are about to usher in a new era of European Data Law. They are interrelated and interlock in various ways.[7] Early in 2023, all five regulations should be available in their final forms. Latecomers were the AIA and the DA, whose initial proposals were unlike DMA, DSA and DGA not presented in November/December 2020, but only in April 2021 and February 2022, respectively.

They will apply additionally to earlier regulative reforms at EU level, especially the transition from the Data Protection Directive to the General Data Protection Regulation in 2018 and the planned transition from the ePrivacy Directive to a proposed ePrivacy Regulation. The constant here is a transition away from regulation (or at least implementation) by the member states towards regulation directly by and from the European Union. All in all, the new European Data Law will not replace established data protection law, but instead exist and apply next to and in addition to data protection law.[8]

However, despite the dominance of EU law in the context of data governance, national German law remains of significance.

[7] *Johannes*, ZD-Aktuell 2022, 01166.
[8] Geminn/Johannes (Eds.), Europäisches Datenrecht, 2023.

1. Data Protection Law

a. The General Data Protection Regulation

Germany has historically been at the forefront of the development of data protection law. The world's first formal data protection law was enacted by the German state of Hesse in 1970. A Federal Data Protection Act followed in 1977. Since 1995, with the European Data Protection Directive,[9] data protection law in Germany has been shaped by a European framework that determines the fundamentals of data protection law in all Member States of the European Communities/Union. This European Directive was replaced by the General Data Protection Regulation (GDPR)[10], which came into effect in 2018. While a directive is a framework that shapes the contents of national law and sets a framework for national lawmakers to act upon, a regulation is directly applicable without the need to enact an implementing act.

However, unlike other regulations, the GDPR still left significant room for the Member States to regulate (making it a "hybrid" between a regulation and a directive in a sense), which resulted in a cooperation between the GDPR and a new Federal Data Protection Act as well as other national data protection acts that still serve as implementing acts even with the GDPR being a regulation.

What must be kept in mind is that despite all modernization that took place since the early days of data protection regulation, data protection law (both in Germany and on the European level, which was heavily influenced by German data protection law) still follows the fundamental principles that were first developed in the 1960s and that formed the basis for the first data protection laws in Germany. This leads to increasing conflicts between these principles, which were originally meant to regulate data processing in few large-capacity computers, and the modern forms and scale of data processing. In their current iteration, these principles are as follows: processing is prohibited unless authorized = lawfulness of processing[11]; fairness; transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.

It must also be kept in mind that the goal of data protection law is the protection of the right of the individual to informational self-determination; the protection of data is only a means to this end.

A general and vital prerequisite for processing personal data is to keep this data secure on a technical and organizational level that is appropriate to the risks resulting from the processing operations. The implementation of data security ("security of processing") is specified in Article 32 GDPR. As a result, data protection and data/IT security go hand in hand.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

[10] 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.

[11] Processing is lawful if the data subject has given consent or if processing is necessary: for the performance of a contract; for compliance with a legal obligation; for the protection of vital interests; for the performance of a task carried out in the public interest or in the exercise of official authority; 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 protection of personal data, in particular where the data subject is a child.

b. The ePrivacy Directive

The Directive on privacy and electronic communications (ePrivacy Directive)[12] is still applicable - despite long-standing efforts to replace it with a regulation. As a directive it had to be adopted into the law of the EU-member states.[13] Besides the GDPR, it is also closely connected to directives and regulations relating to telecommunications, like the European Electronic Communications Code[14].

Efforts to adopt the so-called ePrivacy Regulation that would replace the ePrivacy Directive are ongoing.[15] A first draft was submitted in 2017[16], whereas the current discussion is focused on a draft dated February 10, 2021[17]. The ePrivacy Regulation is intended to focus on dedicated rules for the confidentiality of communications (secrecy of telecommunications), the processing of communications data (previously called "traffic data") and the storage and reading of information on terminal equipment (e.g., so-called "cookies"), thus supplementing the GDPR.

c. The Federal Data Protection Act

Due to the room left for Member States to deviate from, specify or amend the GDPR,[18] national data protection law remains quite significant.

The Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) amends the European data protection law in a few key areas. Some of the most prominent amendments concern criteria for

- video surveillance of publicly accessible spaces,
- processing of special categories of personal data,
- processing of personal data in the context of employment,
- processing for scientific research purposes,
- consumer credits,
- scoring, and
- the rights of the data subject.

d. The Telecommunication-Telemedia Data Protection Act

The Telecommunication-Telemedia Data Protection Act (Telekommunikation-Telemedien-Datenschutz-Gesetz, TTDSG) merges data protection provisions regarding telecommunication and so-called telemedia (a term, which encompasses – among others – a host of internet services)[19]. It transposes the ePrivacy Directive into German law, but it also contains additional provisions. When the ePrivacy Directive will be replaced by a regulation, this act will also need to be overhauled. With regard to telecommunication, the

[12] 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.
[13] E.g., through the German TTDSG, see below.
[14] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
[15] See https://eur-lex.europa.eu/legal-content/DE/HIS/?uri=CELEX:52017PC0010.
[16] Dossier 2017/0003/COD.
[17] Document no. 6087/21.
[18] For more information, refer to *Roßnagel/Bile/Friedewald et al*., Policy Paper 2018.
[19] See the definition in § 1(1) of the Telemedia Act (Telemediengesetz, TMG).

Act seeks to maintain the secrecy of telecommunications.[20] With regard to telemedia, its most impactful provision regulates the use of so-called cookies.[21]

3. The Act on Copyright and Related Rights

The Act on Copyright and Related Rights (Gesetz über Urheberrecht und verwandte Schutzrechte, UrhG) grants authors of works in the literary, scientific and artistic domain protection for their works. Prerequisite for copyright protection[22] as a work is according to § 2(2) UrhG the "*own intellectual creation*". Since those works can be of a digital kind too, special arrangements of data may enjoy protection via the UrhG. As related rights, investments in databases are also protected by the UrhG.

4. The Act on the Protection of Trade Secrets

The Act on the Protection of Trade Secrets (Gesetz zum Schutz von Geschäftsgeheimnissen, GeschGehG) serves to protect trade secrets from unauthorized acquisition, use and disclosure. It is closely linked to data processing operations/systems since insight into certain data might either directly or indirectly reveal know-how and trade secrets and therefore endanger businesses. The GeschGehG is part of the domain of unfair competition law.[23]

5. The Civil Code

The German Civil Code (Bürgerliches Gesetzbuch, BGB) is the central codification of the German general private law, which it forms in combination with ancillary laws. It regulates the legal relationships between private individuals and thus differs from public law. Apart from the general private law it also contains special private rights (Sonderprivatrechte) concerning special subject matters. Rules for all kinds of contracts (e.g., consumer contracts, rules about ownership, possession, or liability rules) can be found in the BGB.

6. The Data Governance Act

The Regulation 2022/868 on European data governance, the Data Governance Act (DGA), was adopted on May 30, 2022.[24] It will be applicable unionwide from September 24, 2023 – with a transitional arrangement for data intermediation services which will have to comply with its provisions by September 24, 2025.[25] The DGA aims to increase trust in data sharing and to thus increase the availability of data for use. It also aims to create new rules on the neutrality of data marketplaces and to facilitate the reuse of certain data held by the public sector. The DGA defines data sharing as the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licenses subject to a fee or free of charge.[26]

---

[20] § 3 TTDSG. See also Article 10(1) GG.
[21] § 25 TTDSG.
[22] Copyright in the subjective sense is the creator's right to his intellectual work, cf. *Rehbinder/Peukert*, Urheberrecht, marginal 4.
[23] It serves to implement Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of confidential know-how and business information (trade secrets) against unlawful acquisition, use and disclosure.
[24] 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.
[25] Cf. Articles 37 and 38 DGA.
[26] See Article 2(10) DGA.

The regulation is specifically concerned with making public sector data available for reuse, sharing of data among businesses (against remuneration in any form), the use of data sharing intermediaries, as well as so-called data altruism. The instrument of data altruism, where data is provided voluntarily, is however limited to purposes of general interest, such as scientific research purposes or improving public services.[27] Regarding data intermediaries, the Commission expects them "*to play a key role in the data economy*".[28] They are made subject to numerous requirements by the DGA and to a central supervision.[29]

7. The Data Act

The proposal[30] for a regulation on harmonized rules for fair access to and use of data (Data Act, DA) was introduced into the official EU legislative procedure on February 24, 2022.[31] It primarily aims to regulate the access to and the use of data by consumers and businesses.[32] Additionally, it would regulate data holders which are legally obliged to make data available.[33] The draft Data Act thus includes provisions for:

- a right of users to access and use user-generated data;
- a ban on unfair contract clauses in standardized data licensing agreements;
- a right to access and use data by public entities;
- a facilitation of switching data processing services (especially cloud and edge providers); and
- requirements for interoperability of data processing services as well as for international data transfer.

Negotiations are ongoing.[34] In all likelihood, consent and adoption will not be reached before 2023. If adopted, the Data Act will probably not enter into force before 2024.

8. The Data Use Act

The Act governing the use of public sector data (Data Use Act, Datennutzungsgesetz, DNG) serves the principle of open data as well as the principle open by design and by default. It is a national German law[35] and only applies to data that are provided by data providers on the basis of a statutory right of access or a statutory duty to provide data, or to data that is otherwise made available to the public or for exclusive use. Data providers according to the DNG are public sector bodies, undertakings providing services of general interest which are subject to the rules on the award of public contracts and concessions or which operate public passenger transport services, as well as universities and researchers.

[27] Article 2(16) DGA.
[28] Recital 27(1) DGA.
[29] See Chapter III DGA: requirements for registration as well as specific requirements for the provision of respective services, such as fair, transparent and non-discriminatory access to these services.
[30] Dossier 2022/0047/COD.
[31] COM(2022) 68.
[32] Chapters II and IV.
[33] Chapter III.
[34] See https://eur-lex.europa.eu/legal-content/DE/HIS/?uri=CELEX:52020PC0767.
[35] It transposes Directive (EU) 2019/1024 on open data and the re-use of public sector information.

9. The Artificial Intelligence Act

On April 21, 2021, the European Commission published a proposal for an Artificial Intelligence Act[36]. The proposal is now being discussed by the EU Parliament and the Council, which represents the EU Member States.

With the Artificial Intelligence Act (AIA), the European Commission was the first lawmaker in the world to attempt to explicitly regulate placing on the market, putting into service and the use of AI systems. The object of regulation is thus not AI as a technology, but instead the application of certain implementations of AI in various contexts. Following a technology-neutral approach, the term AI encompasses certain techniques and approaches, namely machine learning approaches, logic- and knowledge-based approaches as well as statistical approaches – which "*can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*".[37]

Article 10 of the proposed regulation is specifically concerned with data and data governance. In particular, the provisions found here relate to the training of models with data. Data governance thus relates to training, validation and testing data sets here. One of the central principles is that the respective data sets shall be relevant, representative, free of errors and complete.[38]

Negotiations on the AIA are ongoing.[39] If adopted, the AIA will probably apply after two years following the entering into force, so in all likelihood not before 2025.

10. The Digital Services Act

The Digital Services Act (DSA) was adopted on October 19, 2022.[40] It will become applicable by February 17, 2024. However, Article 24(2), (3) and (6), Article 33(3) to (6), Article 37(7), Article 40(13), Article 43 and Sections 4, 5 and 6 of Chapter IV apply since November 16, 2022. The DSA is aimed at providers of intermediary services (e.g., internet service providers, cloud providers, search engines, social networks and other online platforms, and online marketplaces). It covers several issues, including:

- a ban on targeted advertising directed at minors or based on special categories of data;
- a ban on misleading practices and interfaces;
- providing for greater transparency in the parameters for recommending, curating, or prioritizing content for users;
- a commitment to "notice and action" procedures to enable reporting and removal of illegal online content; and
- mandatory "know your business customer" requirements for online marketplaces to ensure merchant reliability.

[36] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence, COM(2021) 206 final.
[37] Article 3(1) AIA.
[38] Article 10(3) AIA.
[39] See https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52021PC0206.
[40] 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).

11. The Digital Markets Act

The Digital Markets Act (DMA) was adopted on September 14, 2022.[41] It applies since May 2, 2023. However, Article 3(6) and (7) and Articles 40, 46, 47, 48, 49 and 50 apply since November 1, 2022 and Article 42 and Article 43 shall apply by June 25, 2023. The DMA is mainly dedicated to the impacts of so-called "gatekeepers" on digital markets. Gatekeepers are providers of core platform services who deliver one of the services listed in Article 2(2) DMA. Among those are for instance online search engines, operating systems, cloud computing services, virtual assistants, and video-sharing platform services. Furthermore, the requirements of Article 3 DMA must be met, which states that a provider for instance must enjoy "*an entrenched and durable position in its operations*" to be classified as a gatekeeper.[42]

The DMA contains certain obligations for such gatekeepers. Some of these obligations are to share data with competitors and other entities. One example is Article 6(11): *"The gatekeeper shall provide to any third-party undertaking providing online search engines, at its request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines. Any such query, click and view data that constitutes personal data shall be anonymised."*

[41] 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 (Digital Markets Act).
[42] Article 3(1)(c) DMA.

B. Data Governance: An Overview of Approaches, Mechanisms and Instruments

The current system of data governance was primarily shaped by data protection law on the one hand and laws regarding intellectual property and regarding the commercial protection of data on the other hand. However, there has always been a vivid discussion in Germany concerning the viability of alternative approaches. With recently enacted or currently proposed European regulations, this discussion as well as discussions in Europe and worldwide were picked up and some of these alternative approaches were given legal standing for the first time. As a result of the evolving European Data Law, some key approaches that were previously discussed as alternatives to established data governance are even very likely to become mainstream.

The following chapters describe select approaches to and mechanisms of data governance as well as instruments of data governance. These approaches, mechanisms and instruments have been clustered according to their primary goal:

- those that primarily aim at enabling or strengthening personal data sovereignty,
- those that can be classified as data intermediation services according to the DGA as well as
- those that meet neither classification.

On the national level, the current coalition agreement states with regard to data governance: *"We elevate the potentials of data for all by initiating the establishment of data infrastructures and instruments like data trusts, data platforms and data donations together with sciences, economy and civil society. We strive for better access to data, in particular to permit start-ups and SMEs new innovative business models and social innovations in digitization."*[43] Consequently, new national laws concerning data governance and amending or complementing the new European Data Law are to be expected in the medium or long term.

One specific area in which data governance has been a subject of intense discussion in Germany is vehicle data. Vehicle data in this context means all data that accumulates from the use of more and more digitized vehicles or traffic infrastructure. One example for the vivid discussion is a report commissioned in 2017 by the Federal Ministry for Transport and Digital Infrastructure[44] concerning an ownership regime for mobility data.[45] Another example is a declaration of intent in the current coalition agreement, which states: *"We establish a Mobility Data Act and secure the free accessibility of traffic data. For the competition-neutral use of vehicle data, we strive for a fiduciary model that appropriately accounts for the access needs of users, private providers and state organs as well as the interest of affected companies and developers."*[46] This is one example for national law in the context of data governance that can be expected in the foreseeable future.

Data governance in the automotive sector is of particular concern in Germany, both because of the importance of the sector for the national economy and because of the many involved actors who claim access rights to the accumulating data – from drivers, vehicle owners or manufacturers to insurances and

[43] Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), 14.
[44] In 2021 renamed to "Federal Ministry for Digital and Transport".
[45] *Denker/Graudenz/Schiff et al.*, in: BMVI 2017.
[46] Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD)m Bündnis 90/Die Grünen und den Freien Demokraten (FDP), 41.

law enforcement agencies. Many general models for an alternative data governance will have to pass a test of compatibility with regard to vehicle data in order to be viable from a German perspective.

I. Data Sovereignty

The term data sovereignty is used in many contexts. Here, it is meant to describe data governance approaches, mechanisms and instruments that are primarily aimed at increasing control over data.

1. Personal Data Sovereignty

One particularly important aspect of data sovereignty is personal data sovereignty, meaning individual control over personal data. Ensuring this personal data sovereignty is the primary goal of the right to protection of personal data, the right to informational self-determination and data protection law. One example of data protection law provisions aimed at supporting the individual by obligating data controllers in this regard is Article 25 GDPR which stipulates data protection by design and by default.

Other examples for ongoing discussions on how to strengthen personal data sovereignty focus around

- a right to switch off data transfers initiated by personally owned digital devices,
- ensuring the security of digital systems and thus of personal data over the entire lifetime of a digital product,[47]
- increasing transparency (e.g., by more clearly communicating to the data subject which data are processed or transmitted), and
- data governance beyond the death of the data subject[48].

Representatives of entities that rely on data processing will often argue against regulation by stressing the importance of the freedom of contract and voluntariness as expressions of individual sovereignty.[49]

2. Use of eID for Identification and Age Verification

In some areas, legitimation checks are required by law before contracts are concluded, for example for financial service providers in accordance with the Money Laundering Act (Geldwäschegesetz, GwG) and also for mobile communications providers in accordance with the Telecommunications Act (Telekommunikationsgesetz, TKG). In other areas, a verification is required by law that a consumer is of a certain age (e.g., sale of alcohol and tobacco, distribution of media that falls under the Youth Protection Act[50]), while others might require the verification of identity and/or age as part of self-imposed business standards. Either way, this may pose a hurdle for internet commerce.

With the online ID card and on-site readout for identification at the point of sale, these requirements can be met very easily and quickly by all parties involved. This allows entrepreneurs to create a seamless conclusion and verification process of contracts via the internet.

---

[47] This is also addressed by the DGA: "Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing." (Recital 39(12) DGA).

[48] See for instance *BGH*, 12 July 2018 – III ZR 183/17 = NJW 2018, 3178; 27 August 2020 – III ZB 30/20 = NJW 2021, 160.

[49] For example bitkom, Stellungnahme Rechtsfragen der digitalisierten Wirtschaft: Datenrechte, 2019, 4.

[50] Jugendschutzgesetz, JuSchG.

In Germany, all citizens above the age of 16 and most long-term residents from outside the European Union are required to apply for a personal electronic identity card (eID) by law.[51] Citizens of the European Union and the European Economic Area can apply for an eID as well.[52]

These eID cards are equipped with a chip that allows for the storage of information. Parts of this information[53] can be read out by using an NFC-reader (e.g., a smartphone with NFC-features) and a software app (i.e., the ID card app issued by the federal government).[54] To use the eID card, software is required to establish a secure connection between the NFC-enabled smartphone or card reader, the ID card, and the eID service provider. It enables an encrypted data exchange between the ID card and the eID service. When using the eID card for identification and authentication, the personal data is transferred directly to the system of the entity asking for identification. They receive verified personal data from the registration authorities and can further process this data within their systems automatically.

The legal basis for integrating the electronic proof of identity with the online ID card into one's own online offerings is the Identity Card Act (Personalausweisgesetz, PAuswG). Authorization to read out eID cards via app is granted by the Authorization Certificate Issuing Office (Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt, VfB) of the Federal Office of Administration. Companies that offer their customers the use of the online ID card in connection with business concerns are referred to as "service providers". The digital offerings with integrated online ID are called "eID services".

There are three different options available for entrepreneurs:

- Entrepreneurs can operate their own eID infrastructure and complete the individual steps to become an eID service provider. This would include to conceptualize the service[55], to apply for issuance of an authorization certificate, to select the provider for the technical authorization certificate, to set up the eID server or select an eID service provider, and to implement the connection of the service to the eID server.
- Entrepreneurs can also get support from eID service providers. They will help obtain the certificates for their eID infrastructure. If required, the eID service providers will also provide the eID infrastructure.
- Entrepreneurs can commission an identification service provider in accordance with § 21 b PAuswG to provide citizen identification as a service for themselves.

3. Data as Compensation

The German Data Ethics Commission (Datenethikkommission, DEK) has adopted a clear stance regarding data as "payment" or "compensation" in the sense of a quid pro quo: "*While the striking denomination has contributed to general awareness, the DEK pleads to desist from describing data as 'compensation'.*

[51] See Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz, PAuswG – Law on identity cards and electronic proof of identity) and §§ 4, 78, 78a Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz, AufenthG – Law on the residence, employment and integration of foreigners in Germany).

[52] See Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis (eID-Karte-Gesetz, eIDKG – Act on a card for citizens of the Union and members of the European Economic Area with an electronic identity verification function).

[53] Family name and first name(s), date and place of birth, address and postal code, if indicated: name at birth, if indicated: order or artist name, if indicated: doctorate.

[54] https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/technik/software/software-node.html.

[55] I.e., which data fields from the eID-card are needed for the electronic proof of identity.

Autonomously from the future interpretation of the so-called 'Kopplungsverbot'[56] *by the supervisory authorities and the ECJ, the DEK postulates that consumers must be offered reasonable alternatives vis-à-vis the dereliction of data for commercial use (e.g., appropriately designed payment models)*."[57]

Regardless of this, the German legislator implemented the European Directive on certain aspects concerning contracts for the supply of digital content and digital services (Digital Content Directive, DCD).[58] As a result, new and special rules for contracts for "digital content and digital services" have applied in German civil law since January 1, 2022. The German legislator has expanded the existing provisions in the German Civil Code on consumer contracts. Specifically, it was added to § 312(1a) BGB that the principles for consumer contracts also apply if "*the consumer provides personal data to the entrepreneur or undertakes to do so*". Paying with data in consumer contracts is therefore allowed by law (while taking into account data protection law). Consent under data protection law and its requirements are quite compatible with the contractual disposal of personal data, as is now possible under §§ 312, 327 BGB.

The provisions of the GDPR retain their full effect. At the same time, it must be kept in mind that the lawfulness of data processing under data protection law does not affect the effectiveness of the contract. This is meant to ensure that the consumer protection provisions of §§ 312 et seq. BGB apply, regardless of whether the entrepreneur adheres to the data protection law or not. The data protection provisions remain in place alongside this (see § 327q BGB). The consumer still has the right and the possibility to revoke consent to data processing, to object to data processing and to exercise his or her data subject rights. Interestingly, the legislator has rejected the widespread view of the so-called "blocking effect of consent". Consequently, the entrepreneur can at least partially "save" the processing of personal data originally based on consent in case of a revocation of consent – e.g., via the legal basis of Article 6(1)(f) GDPR in conjunction with § 7(3) Act against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb, UWG).

Since there are concerns about valuing personal data as "compensation", there are still open questions about the legal form of "payment" with data under the law of obligations and thus under contract law. The Union legislator speaks exclusively of contracts. German law avoids having to draw conclusions about a reciprocal relationship. Therefore, it is not based on a synallagma (do-ut-des) or a conditional linkage but assumes a causal linkage of performance.[59]

In certain cases, the exercise of rights of the data subject granted by data protection law can result in the entrepreneur's right to terminate the contract if the continuation of the contractual relationship is unreasonable. The lack of clarity of the legal concept of unreasonableness has already been criticized in the legislative process.

Transparency and information are key for builders to practically implementable business models and will depend on the design of the respective service package. Information asymmetry, cognitive distortions, and behaviour contrary to preferences must be avoided.

[56] This term, which originates from German contract law, cannot be directly translated into English. Simplified, it means a prohibition to link a contract concerning wares or services with the processing of personal data.
[57] Expert opinion of the German Data Ethics Commission, 2019, 18.
[58] 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.
[59] *Schmitz/Buschuew*, MMR 2022, 171.

5. Ownership of Personal Data?

From the right of informational self-determination derives the authority of the individual to determine the disclosure and use of their personal data. Thus, a self-determined personal development and the self-fulfilment of the individual are protected.[60] At first glance, this seems to imply a form of authority to dispose of one's personal data freely. The idea of data ownership (in relation to personal data) therefore aims at a right of the individual to be able to exclude others from handling their personal data as an absolute right.[61]

However, the authority to dispose one's personal data is actually limited, and the individual is not recognized to have an absolute, unlimitable power of disposing their personal data. One reason for this is the fact that the individual develops their personality in a social community and is dependent on communication.[62] *"Information, even if related to individual persons, represents a reflection of societal reality that cannot be exclusively assigned solely to the parties affected. The Basic Law […] embodies in negotiating the tension between the individual and the Community a decision in favour of civic participation and civic responsibility."*[63] This statement of the Federal Constitutional Court clarifies that an exclusive right for personal data is not acceptable at the level of fundamental rights. Accordingly, informational self-determination tends to be structured as a civil liberty and protects individual freedom, but not rights of disposal.[64]

The Basic Law establishes an objective structural principle which envisages a communication order.[65] This communication order determines who is entitled to access personal data, to handle them, to pass them on or e.g., to restrict their usage.[66] It has its roots in the communicative aspects of all fundamental rights and determines social communication of personal data.[67] This order does not assign exclusive rights, which has implications for data protection law.[68] In the words of the Court: "*Individuals do not have a right in the sense of an absolute, unlimited sovereignty over 'their' data; rather, they are personalities developing within the social community, depending on communication*."[69]

At the European level, the inclusion of data protection in fundamental rights at the European level in Articles 7 and 8 CFR also establishes a right for individuals to determine the processing of their personal

[60] *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, 109.
[61] See *Müller*, DuD 2019, 159 et seq.
[62] BVerfGE 65, 1 (44).
[63] BVerfGE 65, 1 (44).
[64] Also *Denker/Graudenz/Schiff et al.*, in: BMVI 2017, 45.
[65] *Roßnagel,* Datenschutz in einem informatisierten Alltag, 2007, 110 et seq.
[66] *Roßnagel/Jandt/Marschall*, in: Handbuch Industrie 4.0, 2017, Vol. 2 Automatisierung, 491 (493); *Roßnagel,* SVR 2014, 281 (287).
[67] For instance Article 10 GG (Privacy of correspondence, posts and telecommunications), Article 13 GG (Inviolability of the home).
[68] Also *Denker/Graudenz/Schiff et al.*, in: BMVI 2017, 46.
[69] BVerfGE 65, 1 (43 et seq.).

data themselves.[70] Likewise, this right is also considered incompatible with the establishment of an exclusive right in the sense of "data-ownership". Accordingly, the GDPR does not give rise to an exclusive right to personal data either[71] and thus not to data-ownership.

The concept of data ownership has nevertheless gained significant attention in Germany, among other things because of its importance in the context of smart/connected cars.[72] However, in most expert opinions given on data ownership – e.g., the expert opinions of the working group "Digitaler Neustart" (Digital Restart) of the Conference of State Ministers of Justice (2017)[73] and the Data Ethics Commission of the Federal Government (2019)[74] – the idea of data ownership was clearly rejected. Instead, it was expressed that rights to data are already sufficiently protected in various ways in the legal system.

6. Absolute (or Close to Absolute) Rights to Non-Personal Data?

Non-personal data are for obvious reasons also of vital importance for the data economy. One example is the use of machine data in factories at the level of Industry 4.0/the Industrial Internet of Things in the context of predictive maintenance.[75]

There is thus a desire to collect data and evaluate non-personal data with the help of modern methods of analysis and AI. Naturally, this also leads to the desire to be able to exclude others from the handling of this data, as would be the case with factual property.

a. Data as Material Goods?

According to § 903(1) BGB, the owner of a thing (Sache) can, in principle, deal with it at their discretion and exclude others from any influence on it. According to § 90 BGB, things are corporeal (physical) objects in the aggregate states solid, liquid, and gaseous. However, data is not covered by this. A direct application of the ownership regulations for things to data is thus impossible.

A fundamental distinction must be made between data and the ownership of the data carrier/storage medium. The latter is qua corporeality capable of ownership. It (and in consequence the data on it) are protected against tortious effects. As a result, data are not protected via § 823(1) BGB (liability for damages), but the modification or deletion of data on a storage medium leads in case law regularly to the recognition of an infringement of property (and thus liability for damages), since the impairment of the usability fixed in the matter is sufficient.

Still, § 823(1) and (2) BGB do not assign absolute rights to data. Only their protection against tortious impairments is guaranteed, which is fundamentally different in the legal system from an exclusive allocation of goods. With regard to the concept of ownership under civil law, there is therefore no absolute right in the handling of data. This ultimately leads to the conclusion that there is no such thing as data-ownership to non-personal data.

---

[70] *Kingreen*, in: Callies/Ruffert 2022, GRCh Art. 8 marginal 4; *Gersdorf,* in: Gersdorf/Paal 2021, GRCh Art. 8 marginal 4; *Bernsdorff*, in: Meyer/Hölscheidt 2019, GRCh Art. 8 marginal 6 et seq.; Hornung points to this primarily German view and interpretation of Union Law, see *Hornung,* in: Roßnagel/Hornung 2019, 117.

[71] With a differing opinion *Härting,* CR 2016, 646 (648), who in Article 20 GDPR recognizes a first approach of data economization of personal data.

[72] *Denker/Graudenz/Schiff et al*., in: BMVI 2017, 45.

[73] Working group „Digitaler Neustart" (Digital Restart) of the Conference of State Ministers of Justice, 2017, 98.

[74] Expert opinion of the German Data Ethics Commission, 2019, 18.

[75] For data ownership in regard to non-personal data, see *Müller*, DuD 2019, 159 et seq.

b. Data as Copyrighted Works?

Prerequisite for copyright protection[76] is – according to § 2(2) German Act on Copyright and Related Rights (UrhG) – one's "own intellectual creation". Machine data[77] or analyzed smart data[78], e.g., do not meet the requirements for an individual and unmistakable intellectual act of creation, however, because they lack an outstanding degree of individuality and originality (due to their automated generation in sensors or computer programs). The computer program[79] performing the data generation might be able to enjoy copyright protection, but not the generated data.

The individual machine data is also not a database work that could enjoy protection under § 4(2) UrhG as a special case of a collection of works, data or other independent elements (Sammelwerk). The term "database work" describes a collection whose elements are arranged systematically or methodically and the individual elements of which are individually accessible by electronic or other means.

Because of a certain degree of leeway regarding the individual arrangement of the data,[80] data collections can also be protected as database works. Still, this only protects the database itself (as a collection of work), but not the single data or several of them (unstructured). There is therefore protection granted if the database is copied as a whole. If only individual elements are copied and not the structure, copyright protection is not justified per se.[81] The arrangement and selection must, however, be based on the creative activity of a human being, which is not the case with simple automated "filling" of the database with data by machines.[82] The same applies to the automated evaluation of this data.

c. Database Protection according to § 87a et seq. UrhG

In addition to works, certain efforts of investors are also protected. Thus, with regard to a database, the investment made in it and thus the commercial and economic effort is protected by §§ 87a et seq. UrhG by way of an ancillary copyright sui generis.[83] § 87a UrhG limits this to significant investments in the procurement, verification or presentation of the database content. There is no protection regarding investments in data generation.[84]

The maker of this database (Datenbankhersteller) and thus the bearer of the rights under §§ 87a et seq. UrhG is the person who has made the investment or takes the initiative and bears the investment risk.[85] This can be a service provider[86] who operates any corresponding platforms, the entrepreneur who prepares the data of their machine accordingly, the manufacturer of the machine who maintains it and prepares the data for maintenance purposes, or a strategic partner who prepares data stocks in a database

[76] Copyright in the subjective sense is the creator's right to his intellectual work, cf. *Rehbinder/Peukert*, Urheberrecht 2023, marginal 4.
[77] *Peschel/Rockstroh*, MMR 2014, 571 (572).
[78] *Roßnagel,* NJW 2017, 10 (11).
[79] See e.g. *Wiebe*, in: Spindler/Schuster 2019, UrhG § 69a marginal 22 et seq. with further references.
[80] *Marquardt*, in: Wandtke/Bullinger 2022, UrhG § 4, marginal 12; *Dreier*, in: Dreier/Schulze 2022, § 4 marginal 19.
[81] *Wiebe,* in: Spindler/Schuster 2019, UrhG § 4 marginal 14; Collections of work and their content are to be considered legally separate, see § 4 Abs. 1 UrhG.
[82]At most with regard to the computer program underlying the data generation.
[83] *Dreier*, in: Wandtke/Bullinger 2022, UrhG § 4 marginal 9.
[84] *Dreier,* in: Wandtke/Bullinger 2022, UrhG § 4 marginal 8, 12, § 87a marginal 12 ff.
[85] Directive 96/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases, recital 41(2).
[86] *Peschel/Rockstroh*, MMR 2014, 571 (573).

for analysis purposes.[87] In the latter case, the mere provision of the data by the partners cannot be regarded as an investment. Here, the establishment of an operating company may serve the partners involved to overcome this "hurdle".[88]

The producer of the database ("maker") then has the exclusive right under § 87b(1)(1) UrhG to reproduce and distribute the database as a whole or a qualitatively or quantitatively substantial part of the database and to make it available to the public.

d. Data as Trade Secrets?

Machine data and smart data analysis results can also be subject to the protection of unfair competition law if they represent confidential know-how and confidential business information (trade secrets). These are covered by the Act on the Protection of Trade Secrets.[89] "Trade secret" means information (commercial or technical)[90] which meets each 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[91];
b) it has commercial value because it is secret;
c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Whether raw data is covered by the GeschGehG is questionable. Since the protection of secrets is also concerned with protecting investments, not every data or collection of data will be considered as a trade secret, but only such data (sets) which have already reached a certain stage of processing and therefore have an informational value in itself, which in turn can only be considered on a case-by-case basis.[92]

For the owner, however, the trade secret does not constitute an absolute right.[93] As a result, not only can an independent discovery of the same know-how or the same information occur,[94] but an inherent and complete protection of secrets arises in favour of all respective owners.[95]

[87] For more details see *Roßnagel,* NJW 2017, 10 et seq.; *Roßnagel/Jandt/Marschall,* in: Handbuch Industrie 4.0, Vol. 2 Automatisierung, 491 et seq.
[88] *Roßnagel,* NJW 2017, 10 (11). Opposed for the collection of automated data under the database protection law: *Ensthaler,* NJW 2016, 3473 (3478).
[89] This act serves to implement the Directive (EU) 2016/943 of the European Parliament and 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 of 15 June 2016, p. 1).
[90] *Hauck*, in: MüKoUWG 2022, Vol. 2: §§ 7a-20 UWG, GeschGehG § 2 marginal 3.
[91] "Not generally known or readily accessible", the subject of publicity can be both information as such and a value-creating combination of information. Therefore, information is not obvious even if it was known, but no economic exploitability for third parties follows from this. This standard from the old § 17 UWG will have to be applied in this respect. *Hauck*, in: MüKoUWG 2022, Vol. 2: §§ 7a-20 UWG, GeschGehG § 2 marginal 7.
[92] *Hauck*, in: MüKoUWG 2022, Vol. 2: §§ 7a-20 UWG, GeschGehG § 3 marginal 5.
[93] Recital 16 RL (EU) 2016/943.
[94] Article 3 I lit. a RL (EU) 2016/943; § 3 I Nr. 1 GeschGehG.
[95] *Alexander*, in: Köhler/Bornkamm/Feddersen 2022, GeschGehG § 1 marginal 13.

7. Data Possession

Since the legal system in Germany (and the EU) does not yield ownership to data, the idea of data-possession emerged. The concept is derived from the fundamental protection awarded to property/ownership by Article 14 GG, since judicature treats several forms of possession like property/ownership.[96]

In contrast to property/ownership, which in civil law gives an absolute legal position, possession centrally targets the factual dominion over a thing.[97] Someone who, for example, rents an apartment, has a dominion over that apartment. This factual dominion grants a legal position which entails for instance the right to defense against unlawful interference, and the possibility of asserting claims for damages.

So, how does this relate to personal data? § 303a Penal code (Strafgesetzbuch, StGB) threatens punishment to anyone who unlawfully deletes, suppresses, renders unusable or alters data as defined in § 202a(2) StGB. On the flip side, anyone who lawfully handles data does not need to fear punishment. That raises the question in which cases the handling of data is considered lawful. The entitlement to handle data in the context of data possession is seen with the person that writes data onto a storage medium – e.g., into a database. The entitlement of data possession then shall be with the person who has entered the data or created it by executing a program.[98] As a result, the possibility of being able to handle the data in accordance with a factual dominion is to be equivalent to a factual dominion under civil law and, in this respect, establishes a protected legal position.

8. Data Portability and Interoperability

Data portability can also be understood as an instrument of data governance. It is an obligation to provide access to data and results in the need to provide interfaces for export and import of relevant data.

The GDPR contains a right to data portability in Article 20. Under certain conditions[99] the data subject has "*the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and ha[s] the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided*".[100] This right is mostly geared towards enabling users to transfer user profiles from one social network to another, but it also applies in similar contexts (e.g., switching from one email provider to another).

According to Article 6(9) DMA gatekeepers have the obligation to provide end users and third parties authorized by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data. Furthermore, gatekeepers shall allow providers of services and providers of hardware, free of charge, effective interoperability with their systems within the limits of Article 6(7) DMA.

[96] *Michl*, NJW 2019, 2729; *Hoeren*, MMR 2019, 5.
[97] *Hoeren*, MMR 2019, 5.
[98] *Hoeren*, MMR 2019, 5 (7).
[99] The processing is based on consent or necessary for the performance of a contract and carried out by automated means.
[100] Article 20(1) GDPR.

Under the proposed Data Act these rights and obligations would be strengthened and expounded on by defining essential requirements regarding interoperability (Article 28 and 29 DA) and provide for the development of interoperability standards for data to be reused between sectors.

9. Voluntary Provision and Sharing of Data

The voluntary provision of (usually personal) data was recently widely discussed in the context of the COVID-19 pandemic under the term "data donation". In the meantime, the DGA has established the term "data altruism" as a specific concept for the voluntary provision of both personal and non-personal data.

a. Donation of Personal Data

Especially in medical research, the reuse/secondary use of patient data is of significance[101], as was confirmed by an expert opinion for the Federal Ministry of Health.[102] However, legal (data protection requires special care when processing of special categories of personal data like health data) and technical (e.g., data quality, distributed systems and incompatible formats) hurdles are impeding the free use of these personal data.

Although anonymization of personal data eliminates the data protection concerns in most cases (notwithstanding the problem of re-identification), the possibility to assign data to a specific person is often desired, "*since e.g. long-term studies require a continuous assignment of new data to already existing data*".[103]

In Germany, data-donation as a concept became widely known during the coronavirus pandemic when the Robert-Koch-Institut (RKI) – the government's central scientific institution in the field of biomedicine and one of the most important bodies for the safeguarding of public health in Germany – as the official publisher of the Corona-Warn-App (Germany's official COVID-19 contact tracing app) offered an additional mobile app for donating personal health data from smartphones or other connected wearables for research purposes in relation to the pandemic.[104] However, this was not the first time that the concept of data donation was discussed in the context of public health.[105]

As with all other forms of personal data for commercial use in big-data-applications, health data is also "*a continuous source-of-insight for research, that only rarely loses its scientific value. Many scientific questions, which could be edited with the help of these data, are not even exactly known at the time of their collection*".[106]

Three forms of lawful utilization in the framework of the donation of medical/health data are taken into account by the aforementioned expert opinion:

[101] E.g., *Petri*, DuD 2022, 413 et seq.
[102] *Strech/Graf von Kielmansegg/Zenker*, „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen 2020.
[103] *Strech/Graf von Kielmansegg/Zenker*, „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen 2020, 41.
[104] COVID-19 contact tracing app, https://corona-datenspende.de/.
[105] Cf. *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018.
[106] *Strech/Graf von Kielmansegg/Zenker*, „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen 2020, 42.

1. The free permission for the processing of personal data, in particular health data, for the purposes of research, to third parties. This would require prior information to the person about the nature, purpose and scope of the processing as well as the associated risks for him.[107] Corresponding consent would have to be given, which includes the risk of said consent being revoked at a later point in time. Another issue lies with the limitation of purpose (as stipulated by the principles relating to processing of personal data due to Article 5 GDPR), even where broad consent is given. This leads to the request for area-specific openings to enable data donation without this limitation.[108]
2. The utilization of data could also be based on the legal permission embedded in Article 9(2)(j) in connection with 89(1) GDPR which could replace any consent. These provisions authorize the national legislator to draft a norm that would allow the utilization of data for research purposes without consent, if the public interest concerning the goal pursued by the processing outweighs the risks resulting from the processing of the data and appropriate safeguards are installed. Neither the GDPR nor the German national law so far stipulates, at which point such a weighing of interests should take place, i.e. who would have to decide on the admissibility of the use of the data for a specific research purpose. It has been proposed "*to bundle the necessary expertise in independent, locally operating committees (Use and Access Committees, UAC) and to assign them the appropriate approval or veto rights for the use of data by law in dependence of the sensibility of each research project*".[109] In addition, a publicly accessible research register could be created in which the use of personal medical/health data would be documented summarily on a project-by-project basis.
3. The expert opinion also proposes the creation of a relevant norm on the permitted use of such medical/health data for research purposes, which will define all the rights and obligations of the parties involved – including the possibilities for data donors to participate and the conditions for data use by researchers.[110] It should also include the possibility for data subjects to opt-out.

The term "donation" normally implies that something is provided voluntarily and purposefully. Only options 1 and 3 would meet this definition – and the latter only if it envisages a possibility to opt-in, since opting-out is not seen per se as a legal way to process data whereas opting-in is. Option 2 would only be a "donation" by name. The authors of the expert opinion do (according to option 1 and 3) define data donation in the context of research with medical/health data as a "*voluntary and informed granted consent that specific personal medical data may be processed by third parties for purposes of research in a legally compliant manner as long as the processing meets the conditions attached to the donation*".[111]

b. Data Altruism

Under the DGA data altruism can mean two different things.[112] On the one hand, it is the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them (i.e., Data Donation, see above). On the other hand, data altruism also means permissions of data holders to allow

[107] For this and the following see *Strech/Graf von Kielmansegg/Zenker,* „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen 2020, 45 et seq.
[108] *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, 266 et seq.
[109] *Strech/Graf von Kielmansegg/Zenker*, „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen 2020, 46.
[110] *Strech/Graf von Kielmansegg/Zenker*, „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen 2020, 46.
[111] *Strech/Graf von Kielmansegg/Zenker*, „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen 2020, 46 et seq.
[112] See Article 2(16) DGA.

the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law. Such national law may for instance relate to healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest.

II. Data Intermediation Services

The DGA has established the term "data intermediation services" as well as a notification and supervisory framework for the provision of such services.[113] As a regulation, the DGA is directly applicable in the EU member states without the need for an implementing act.

Article 2(11) DGA defines a data intermediation service as a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other. As a result, services which establish non-commercial relationships are not categorized as data intermediation services for the purposes of the DGA. The data sharing can be facilitated through technical, legal, or other means, including for the purpose of exercising the rights of data subjects in relation to personal data. Data intermediation services are by definition not and may not include:

- 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,
- services that focus on the intermediation of copyright-protected content,
- 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 as well as,
- data sharing services offered by public sector bodies that do not aim to establish commercial relationships.

This means that data brokers (i.e. companies that purchase data from a large number of companies in order to process it and then sell it on to other companies) are therefore not regulated as data intermediation services by the DGA.[114] Service providers for the sharing of online content pursuant to Article 2(6)[115] Copyright Directive[116] are also expressly excluded.[117] The same is true for closed data platforms, in which

[113] Article 1(1)(b) DGA.
[114] *Hennemann/von Ditfurth*, NJW 2022, 1905 (1908).
[115] "'online content-sharing service provider' means a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes. Providers of services, such as not-for-profit online encyclopedias, not-for-profit educational and scientific repositories, open source software-developing and-sharing platforms, providers of electronic communications services as defined in Directive (EU) 2018/1972, online marketplaces, business-to-business cloud services and cloud services that allow users to upload content for their own use, are not 'online content-sharing service providers' within the meaning of this Directive."
[116] 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.
[117] Recital 29 DGA.

only a predefined group of companies may participate. Similarly, platforms through which only one company shares its data with other companies do not fall within the scope of the DGA.[118] An example for the latter is the B2B platform BMW Car Data, through which access to data of BMW vehicles can be acquired.[119]

Article 10(a)-(c) DGA lists three types of data intermediation services which are subject to the provisions in Chapter III DGA: (a) intermediation services between data holders and potential data users; (b) intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make non-personal data available, and potential data users; (c) services of data cooperatives.

Data intermediation services are not limited to personal data; data that has no personal references and is thus outside the scope of data protection law may also be shared. The DGA names a few examples for data intermediation services, e.g.[120]:

- data marketplaces, on which undertakings could make data available to others,
- orchestrators of data sharing ecosystems that are open to all interested parties, for instance in the context of common European data spaces,
- data pools established jointly by several legal or natural persons with the intention to license the use of such data pools to all interested parties in a manner that all participants that contribute to the data pools would receive a reward for their contribution.

Data intermediation services are generally subject to a notification procedure (Article 11 DGA) and certain conditions according to Article 12(a)-(o) DGA that must be met. They are exempt from the aforementioned requirements (Article 15 DGA), if they are recognized data altruism organizations or other not-for-profit entities insofar as their activities consist of seeking to collect data for objectives of general interest, made available by natural or legal persons on the basis of data altruism. This exemption does not apply, if those organizations and entities aim to establish commercial relationships between an undetermined number of data subjects and data holders on the one hand and data users on the other.

1. Data Trusts/Data Fiduciaries

The group of phenomena often referred to as “data trusts” or as “data fiduciaries” can be structured as a three-sided constellation: There are several “data providers” (1) who transmit data to a “data trustee" or “data fiduciary” (2) who bundles it and, if necessary, processes it further (e.g., anonymizes it or processes it in some other way) and makes it available to one or more “data users" (3). There can, but need not be, a difference in persons between “data providers” and “data users”. In contrast to this, a “data trader” can be understood as someone who buys data in order to use them as their own goods, especially to exploit them for their own benefit. The “data trustee” or “data fiduciary”, however, works for the benefit of others, in particular for the interest of the “data provider”; they have to live up to the trust invested into the service and treats the data as third-party goods, i.e., as fiduciary property.[121]

A broad definition of “data trust” or “data fiduciary” might be: A natural or legal person or a partnership that mediates access to data provided or held by a “data trust” or an “data fiduciary” in accordance with

[118] Recital 28 DGA.
[119] *Hennemann/von Ditfurth*, NJW 2022, 1905 (1908).
[120] Recital 28(4) DGA.
[121] *Kempny/Krüger/Spindler*, NJW 2022, 1646 et seq.

contractually agreed or legally prescribed data governance regulations (also) in the interests of third parties.[122] One of the definitions that are proposed define it as a "*natural or legal person or a partnership that mediates access to data provided or held by data trustors in accordance with contractually agreed or legally prescribed data governance rules in the interest of others*".[123]

Data fiduciary models have in common that fiduciaries act as intermediaries for the purpose of data sharing or data access.[124] Since engaging in this activity lies in the interest of a third party it thus falls within the scope of an order or agency agreement under German civil law (§§ 662, 675 BGB). Even though similarities to "real" fiduciaries can be found here, data fiduciary models do not establish a "real" fiduciary relationship in that sense. Nevertheless, the are characterized by the central obligation to implement the sharing or access under the trustor´s specifications towards data users.[125]

Neither the term data trust nor the term data fiduciary are defined by law.[126] They are placeholders or generic terms for various business models and means and ways of data sharing. In lieu of definitions, the terms can be used interchangeably.[127]

A systematization of data fiduciary/trusts models can be made according to their purpose. Management functions (see PIMS below), voluntary self-restraint, and the solving of access problems as a systematic classification of purposes, as well as optional data caches and hosts and mandatory data caches and hosts as risk-based regulatory models are commonly mentioned.[128]

Voluntary self-restraint is aimed at restricting a data processor by the fiduciary (who takes over the management of the controller's data) and controls their access to it. The fiduciary checks whether the access requirements are met and allows access only within the scope of the authorization.

Solving a so-called "real data access problem"[129] distinguishes three scenarios: The intermediation in the interest of the data subject (following the example of Article 10(b) DGA) (1), in the interest of the data holder (following the example of Article 10(a) DGA) (2) and a double-sided fiduciary (3).

In the intermediation interest of the data subject (trustor), the fiduciary is proposed as a strong intermediary who compensates existing power asymmetries and enforces compliance with the requirements of the data subjects. To this end, it implements the requirements of data protection law, grants third parties controlled access to personal data, negotiates access conditions to the data and monitors compliance with them.[130]

The fiduciary is proposed as the one who de facto holds and manages the data of the trustor. The concept is intended to ensure the exchange of data within the framework of the specifications and in the interest of the data processor. However, it is also conceivable that the purposes of the data trust will benefit both the interests of the data subjects and of the data processor in a cumulative model, for instance in the case that the data may be processed by the data processor for specific purposes in a protected area ("data

[122] *Blankertz/Specht-Riemenschneider*, Neue Modelle ermöglichen – Regulierung für Datentreuhänder, 2021.
[123] *Specht-Riemenschneider/Blankertz/Sierek et al*., Die Datentreuhand, MMR-Beilage 2021, 27.
[124] *Specht-Riemenschneider/Blankertz/Sierek et al.*, Die Datentreuhand, MMR-Beilage 2021, 26.
[125] *Specht-Riemenschneider/Blankertz/Sierek et al.*, Die Datentreuhand, MMR-Beilage 2021, 26 et seq.
[126] However, "fiduciaries" and "trusts" are different legal entities, especially in common law.
[127] While "data trust" seems to be the more generic term and more generally used, "fiduciary" is used in Recital 33 DGA.
[128] Read more at *Specht-Riemenschneider/Blankertz/Sierek et al*., Die Datentreuhand, MMR-Beilage 2021, 27 et seq.
[129] Read more at *Specht-Riemenschneider/Blankertz/Sierek et al*., Die Datentreuhand, MMR-Beilage 2021, 28 et seq.
[130] *Specht-Riemenschneider/Blankertz/Sierek et al*., Die Datentreuhand, MMR-Beilage 2021, 28.

room") of the fiduciary for certain purposes (double-sided fiduciary). In this scenario, the fiduciary ensures compliance with the requirements of the data subject and allows data to be handled for defined purposes in a secure environment in his sphere.[131]

A systematization of data fiduciary/trusts models can also be made according to their risks. This helps to identify regulatory needs.[132] A distinction can be made between mandatory and optional use with mandatory use always requiring regulation. Furthermore, a distinction can be between central storage (by the data fiduciary) or decentralized storage (by the data processor or data subject) as well as a transmission of the data (by the data fiduciary).

The differences regarding the type of storage either lead to the scenario of a data room ("data host") or of a pure data transmission instance ("data cache"). Some types of data have higher protection requirements than others (e.g., from commercial confidentiality, including business, professional and company secrets; statistical confidentiality; the protection of intellectual property rights of third parties; the protection of personal data which favors a risk-based approach).

So-called "data trusts" or "data fiduciaries" are classified as data intermediation services, if the aforementioned criteria are met. It has to be noted, however, that other forms of "data trusts" or "data fiduciaries" are not subject to the provisions in Chapter III DGA.

2. Data Cooperatives

A data cooperative is a special form of data intermediation service which has been regulated for the first time by the DGA. The goal of data cooperatives is, among others, to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organizations attached to data use to give better choices to the individual members of the group or potentially finding solutions to conflicting positions of individual members of a group on how data can be used where such data relates to several data subjects within that group.[133]

Article 2(15) DGA defines "services of data cooperatives" as data intermediation services offered by an organizational structure constituted by data subjects, one-person undertakings or SMEs[134] who are members of that structure. This structure must have as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data.

Each individual member of the cooperative simultaneously provides data and in return benefits from the data provided by the other members. The purposes of the data usage are defined jointly within the data cooperative. The idea of data cooperatives is still a topic of research. Possible areas of application arise in manufacturing and in the service sector, for example in banking, logistics or tourism.

[131] *Specht-Riemenschneider/Blankertz/Sierek et al.*, Die Datentreuhand, MMR-Beilage 2021, 29.
[132] *Specht-Riemenschneider/Blankertz/Sierek et al.*, Die Datentreuhand, MMR-Beilage 2021, 29 et seq.
[133] Recital 31 DGA.
[134] Small and medium-sized enterprises.

3. Data Marketplaces

Data marketplaces are marketplaces on which undertakings could make data available to others.[135] Users of such a marketplace can thus buy and sell data to other users; the provider of the marketplace itself does not necessarily provide any data for sale. The provider of the marketplace thus only provides a digital infrastructure for the sale of data. A data marketplace could be structured in a centralized way (using a central platform) or a decentralized way (e.g., using blockchain technology).

4. Data Pools

A data pool is commonly used for sharing data among multiple users and/or devices within one organization. That organization is then the controller. Data sharing pools are commonly viewed as a solution to break open data silos. Data silos are understood as closed sets of data which stand side by side without internal connection and can only be used by a limited group or department of a company.[136] From the company's point of view, the data thus loses value because it cannot be used efficiently for business purposes. Data silos often develop when different departments within a company use different data processing structures and isolated software solutions without sufficient interfaces to exchange data sets. Data silos are thus the result of companies introducing different software solutions for different purposes over time. With a company-wide data sharing pool the company's data sets can supposedly be used much more efficiently.

Multilateral and multiorganizational data pools might be organized as data intermediation services (see above). These data pools could be established jointly by several legal or natural persons with the intention to license the use of such data pools to all interested parties in a manner that all participants that contribute to the data pools would receive a reward for their contribution.[137]

5. European Data Spaces

Data intermediation services could function as orchestrators of data sharing ecosystems that are open to all interested parties.[138] In order to support the free and safe international flow of data, the European Commission proposed establishing domain-specific common European data spaces for data sharing and data pooling. Specific data sharing pools are the common European Data Spaces defined by the European strategy for data as of February 2020.[139] They aim at ensuring that more data becomes available for use within the economy and within society, while keeping companies and individuals who generate the data in control. The nine initial Common European Data Spaces include the following sectors: industrial and manufacturing, Green Deal, mobility, health, finance, energy, agriculture, public administrations, and skills.[140] The European Commission already proposed a Regulation on the European Health Data Space in 2022[141] and will further report on the development of Common European Data Spaces in 2023.

---

[135] Recital 28(4) DGA.
[136] *Rashedi*, Was ist ein Datensilo?, 2020; *Janzen*, Das Problem von Datensilos – und wie gutes Datenmanagement diese aufbricht, 2021.
[137] Recital 28(4) DGA.
[138] Recital 28(4) DGA.
[139] European strategy for data, https://digital-strategy.ec.europa.eu/en/policies/strategy-data.
[140] http://dataspaces.info/common-european-data-spaces/#page-content.
[141] COM (2022) 197; see also https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52022PC0197.

6. Personal Information Management System (PIMS) Providers

PIMS can help the data subject to exercise control over their data by implementing their requirements towards data users automatically. This can also be offered as service. The management function of the service would consist of the mediation of the data in the interest of the data subject to data processors with whom the data subject negotiates access contracts, including for example the monetization of the data and the data subject's participation in it.

Such services might be facilitated via software agents. Software agents can be used to support the individual in the context of data control. There are two main scenarios: (1) In the first scenario, a software agent automatically performs an evaluation of privacy policies or of digital services, products or websites and give feedback to the user. The user can then decide whether or not to use a service or product based on the information provided by the software agent. (2) In the second scenario, preferences regarding data processing are fed into a software agent. The agent can then automatically communicate these preferences to a digital service or a website and request respective changes to the data processing activities.

Regulated under German law are PIMS regarding cookies. By means of cookies and similar technologies, information can be stored, enriched and managed directly on the devices of users. When used with unique identifiers (UIDs), this permits identification or assignment to a natural person. In practice, these processes are often used to track the individual behavior of users – in some cases across different websites and devices – and, if necessary, to create profiles of a person.

The lawfulness of these (subsequent) processing operations is governed by the requirements of the GDPR. However, the upstream technical processes – in particular the setting and reading of cookies – also affect the integrity of the terminal equipment and thus originally fall within the scope of Directive 2002/98/EC as amended by Directive 2009/136/EC (so-called “ePrivacy Directive”, see above). Effective December 1, 2021, Article 5(3) of the ePrivacy Directive was transposed into German law by § 25 Telecommunications Telemedia Data Protection Act (TTDSG), which must be observed when using any technologies by means of which information is stored on or read from terminal equipment.

Article 5(3)(1) of the ePrivacy Directive was transposed into national law in § 25(1)(1) TTDSG. In contrast to the ePrivacy Directive, the TTDSG also contains a special provision for PIMS. Specifically, so-called services for the administration of acts of consents granted under § 25 TTDSG can seek government recognition. However, there is no general recognition obligation for PIMS providers. § 26 TTDSG is intended to provide them with a secure and enabling legal framework.[142]

Requirements for recognition include that the services do not pursue any economic self-interest and that their data processing is limited to consent management purposes (§ 26(1)(2) and (3) TTDSG). A commercial PIMS provider offering is possible, since the prohibition of economic self-interest relates to data exploitation and not to consent management as such. To flesh out the recognition requirements in more detail, the enactment of a statutory ordinance is planned (§ 26(2) TTDSG).[143]

§ 26 TTDSG does not give any details on digital consent assistance itself. § 26(1)(1) TTDSG merely clarifies that the standard applies to services that enable consent to be obtained and managed. However, it remains unclear under which conditions an automated declaration of consent is permissible. The explanatory memorandum only states that consent management services are already “possible under the current

[142] BT-Drs. 19/29839, 68.
[143] For further information see *Nebel*, ZD-Aktuell 2022, 01321.

legal situation".[144] Whether this legal opinion is convincing depends on the interpretation of the GDPR, to which Section 25(1)(2) TTDSG also refers.

III. Other Data Sharing Models

1. Open Data

There is no legal definition of "open data", not even in the Open Data Directive.[145] Open data can, however, be understood as data that can be freely used, re-used and redistributed by anyone – subject only (at most) to the requirement to attribute and share alike.[146]

The full Open Definition by the Open Knowledge Foundation gives precise details as to what this might mean:[147]

- Availability and Access: the data must be available as a whole and at no more than a reasonable reproduction cost, preferably by downloading over the internet. The data must also be available in a convenient and modifiable form.
- Re-use and Redistribution: the data must be provided under terms that permit re-use and redistribution including the intermixing with other datasets.
- Universal Participation: everyone must be able to use, re-use and redistribute - there should be no discrimination against fields of endeavour or against persons or groups. For example, "non-commercial" restrictions that would prevent "commercial" use, or restrictions of use for certain purposes (e.g., only in education), are not allowed.

The idea behind the concept is to establish an obligation (mostly without presuppositions) to share data that are not subject to overriding rights.

Creative Commons or other Open Sources Licenses can be used to share data. Creative Commons licenses are standard licenses that have become established worldwide for licensing "free content" (open content). They are based on the basic idea that creators or owners often have a need or a desire to open up more extensive use of their content than permitted by law itself, without having to transfer rights of use in each individual case. Creative Commons and other Open-Source Licenses are in principle compatible with German laws on intellectual property, copyright, and related rights.

2. Legal Obligations to Share Data

Legal obligations for corporations to share their data are considered to make inadequately used data stocks more useful and at the same time provide innovation incentives for small and medium sized companies by breaking up dominant market positions of large corporations.[148] However, the proposal for a "data-for-all" Act failed. As it stands, only antitrust law contains provisions that obligate companies to share data under certain conditions. Pursuant to § 19a(2) No. 5 of the Act against Restraints of Competition (Competition Act, Gesetz gegen Wettbewerbsbeschränkungen, GWB), the German Federal Cartel Office (Bundeskartellamt) is authorized to prohibit market-dominating companies from refusing or impeding

[144] BT-Drs. 19/29839, 67.
[145] 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.
[146] „What is Open Data?", https://opendatahandbook.org/guide/en/what-is-open-data/.
[147] Open Definition 2.1, https://opendefinition.org/od/2.1/en/.
[148] For the Social Democratic Party's proposal for a legal obligation to share data see in detail *Geminn*, ZD-Aktuell 2019, 06492.

the interoperability of products or services or the portability of data. The Federal Cartel Office can therefore use a prohibition order to force companies to share data in order to ensure interoperability and portability.

In addition, § 20(1) and 20(1a) GWB prohibits market-dominating companies from denying other competitors access to data controlled by the market-dominating company if these competitors are dependent on access to data for their own activities. That is the case if competitors are dependent as suppliers or consumers of a certain type of goods or commercial services in such a way that there are no sufficient and reasonable possibilities of switching to third companies and if there is a clear imbalance between competitors and market-dominating companies. If these requirements are met, market-dominating companies can be forced by the Federal Cartel Office to share certain data which those companies control.

The existing data sharing obligations under antitrust law are rather limited in comparison to the obligations set by the Digital Markets Act. When the DMA comes into effect, such obligations will be significantly expanded beyond the scope of antitrust law. In any case, data sharing must comply with all data protection requirements of the GDPR and national data protection laws. It is unclear whether and, if so, under what conditions §§ 19a, 20 Competition Act will apply at all after the DMA comes into effect. In principle, this depends on whether the DMA enjoys priority of application or the national law remains applicable due to an opening clause. Because this is a highly controversial topic, it will ultimately have to be determined by the European Court of Justice.[149]

3. Processing on Behalf of a Controller and Joint Controllers

The shift away from in-house hardware and software and towards cloud-based resources continues unabated. Software, infrastructure, and platforms as a service can give momentum when starting a business. Digital services other than cloud-services are also offered in different kinds and shapes.

Data processing on behalf of the controller thus becomes more and more the rule for business-starters. Sometimes it is not even evident that an outsourced data processing occurs. For example, using Microsoft-365 or Office-365 online regularly bears the risk of outsourcing data processing of personal data into cloud environments (software as a service[150]). Having a website hosted[151] and implementing forms of third-party analysing tools[152] leads to situations of processing on behalf of the controller as well.

This has legal implications: Since business-starters remain data controllers with regard to the outsourced processing of personal data and the use of digital and "…-as-a-service" services regularly constitutes data processing on behalf of the controller, there should be a high level of interest on their part to keep in compliance with the requirements set forth in the GDPR. The interest originates from the controller remaining liable in relation to the data subject in the event of a breach of the requirements of the GDPR by the processor, which may result in fines and other penalties (Articles 83, 84 GDPR in connection with §§ 41 et seq. Federal Data Protection Act).

Data processing on behalf of the controller is regulated by Article 28 et seq. GDPR. These provisions obligate the controller, e.g., to use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. As a result, the controller must select

[149] In detail see Scientific Service of the German Parliament, WD 7 - 3000 - 114/21; PE 6 - 3000 - 067/21.
[150] *Völker/Schnatz/Breyer*, MMR 2022, 427 (428); *Sörup/Parvez*, ZD 2021, 291 (292).
[151] *Krasemann*, in: Jandt/Steidle 2018, part B II. marginal 178.
[152] *Krasemann*, in: Jandt/Steidle 2018, part B II. marginal 180.

and monitor the processor carefully in order to be secure that they comply with the obligations that rest with the controller when processing personal data.

Data processing on behalf of the controller differs from the so-called "joint controllership" in Article 26 GDPR. For example, if someone starting a business implements social plugins in their website, this establishes a joint controllership with the social media platform provider,[153] meaning that they are directly liable, since they are not outsourcing their processing operations but jointly deciding with the plug-in-provider the purposes of the processing operations of collection of the personal data and the disclosure by transmission.

4. Data Brokers

Data brokers specialize in collecting data (personal or non-personal) in order to aggregate, enrich or transform that data and sell or license that obtained information to third parties. The data may be collected for example from public records, via webtracking or through loyalty cards or purchased from companies. Data brokers are not considered to be data intermediation services as defined by the DGA.[154]

A wide range of data brokers exist. For example, the economy depends on reliable information to determine whether a person is creditworthy or not. The determination of creditworthiness and the provision of credit reports are the foundation of the German credit system and thus also of the functioning of the economy.[155] Data brokers in this particular context are called "Auskunftei", i.e. "credit reporting agency". Such an agency is a company that (irrespective of the existence of a specific inquiry) collects creditworthiness-related data on companies or private individuals in order to make it available to its business partners (if required) for the purpose of assessing the creditworthiness of the persons concerned in return for payment.[156] In addition to the individual data, credit agencies also compile and pass on so-called score values.[157]

Since this kind of data processing creates the risk of profiling data subjects in regard to possibly sensitive kinds of data, additional requirements in order to protect them have been introduced. § 31 BDSG specifically aims at the "*Protection of commercial transactions in the case of scoring and credit reports*". § 31(1) BDSG[158] contains the requirements for data protection-compliant scoring and specifies (with regard to § 31(2) BDSG[159]) the requirements that a score determined by a credit reporting agency must meet with

[153] *ECJ*, ECLI:EU:C:2019:629 para. 81 (Fashion ID).
[154] Recital 28 DGA.
[155] BT-Drs. 18/11325, 101.
[156] BT-Drs. 16/10529, 9.
[157] *Duhr*, in: Roßnagel 2003, 1172 para. 48.
[158] For the purpose of deciding on the creation, execution or termination of a contractual relationship with a natural person, the use of a probability value for certain future action by this person (scoring) shall be permitted only if 1. the provisions of data protection law have been followed; 2. the data used to calculate the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognized mathematic-statistical procedure; 3. other data in addition to address data are used to calculate the probability value; and 4. if address data are used, the data subject was notified ahead of time of the planned use of these data; this notification shall be documented.
[159] The use of a probability value calculated by credit reporting agencies to determine a natural person's ability and willingness to pay shall be permitted in the case of including information on claims only as far as the conditions of subsection 1 are met and only claims concerning a performance owed which has not been rendered on time are considered 1. which have been established by a final decision or a decision declared enforceable for the time being, or if an executory title has been issued under Section 794 of the Code of Civil Procedures, 2. which have been established under Section 178 of the Insolvency Act and have not been disputed by the debtor at the verification meeting,

regard to so-called negative features (Negativ-Merkmale) in order to be registered and used in commercial transactions.[160]

5. Processing of Anonymized Data

Anonymization is usually regarded as a highly effective measure to avoid strict data protection provisions and to freely be able to process formerly personal data. However, due to technological progress there remains always a risk that anonymized data may be de-anonymized at some point in the future, making re-identification of the data subject possible. To address this risk, there are calls to make applicable select data protection law provisions not only to personal data, but also to anonymized data.[161]

In lieu of such a legal framework specific to the processing of anonymized data, processors could choose to adhere to select data protection law provisions on a voluntary basis or draw up their own set of rules. Examples could be an explicit ban on deanonymization, clear and concrete rules on anonymization procedures, rules on purpose limitations, transparency rules and rules on the deletion of anonymized data.[162] These rules could even be institutionalized in the form of a certificate that demonstrates the implementation of (legally not required) safeguards when processing anonymized data.

A possible benefit could be an increase in trust in the processing of anonymized data which could in turn boost the use of artificial intelligence and big data by minimizing risks and liability when sharing anonymized data.

6. Public Data Trusts / Re-Use of Data Pursuant to DGA

The term "public data trusts" broadly refer to a model of data governance in which a public actor accesses, aggregates and uses data about citizens, including data held by commercial entities, with which it establishes a relationship of trust.[163] The term is not legally defined. Public data trusts can be data intermediation services in the sense of the DGA, if they offer their services commercially.

The DGA provides specific rules for the re-use of data held by public sector bodies. The idea behind this is that data generated or collected with the help of public funds should also benefit society (Recital 6 DGA). Chapter II of the DGA sets out the conditions for the further use of specific data that is held by public bodies and that is protected for certain reasons. Article 3(1) DGA conclusively lists business secrecy (including trade, professional and company secrets), statistical secrecy, the protection of the intellectual property of third parties and the protection of personal data as grounds worthy of protection. According to Article 7(1) DGA, member states shall designate one or more competent bodies, which may be competent for particular sectors, to assist the public sector bodies which grant or refuse access for the re-use of data. These competent bodies would constitute public data trusts.

---

3. which the debtor has explicitly acknowledged, 4. for which a) the debtor has received at least two written reminders after the due date of the claim, b) at least four weeks have elapsed since the first reminder, c) the debtor was previously informed, at least in the first reminder, of possible consideration by a credit reporting agency and d) the debtor has not disputed the claim, or 5. the contractual relationship on which the claim is based can be terminated without prior notice for payment in arrears and the debtor has been informed of possible consideration by a credit reporting agency.

[160] *Taeger*, RDV 2017, 3 (4).

[161] See for instance *Roßnagel/Geminn*, ZD 2021, 487.

[162] Cf. *Roßnagel/Geminn*, ZD 2021, 487 (490).

[163] *Micheli et al.*, Big Data & Society 7, Nr. 2 (July 1, 2020): 2053951720948087.

7. Data Trusts/Fiduciaries and Other Services Not Classified as Data Intermediation Services

Only those data trusts/fiduciaries and other services that meet the criteria set forth in Articles 2(11) and 10 DGA are classified as data intermediation services and are thus subject to the provisions of Chapter III DGA. Besides the four examples for excluded services listed in Article 2(11) DGA, all types of services are excluded which do not aim to establish commercial relationships. Not-for-profit trusts and fiduciaries for instance may thus operate beyond the restrictions and obligations of data intermediation services.

C. Summary

Lawful data governance requires ongoing monitoring and review to ensure that data management practices remain compliant with changing legal and regulatory requirements.

Germany presents a complex legal framework for data governance – through directly applicable EU legislation, transposed EU legislation as well as national laws. This legal framework or environment contains guidelines and enables opportunities for data governance approaches that strengthen data sovereignty, but it also stipulates restrictions and bureaucratic requirements that may feel overwhelming at first glance. These restrictions are however meant to serve the interests of data subjects, data providers and data holders alike.

This is especially important in the context of sharing data among organisations. Sharing data can bring numerous economic benefits, including increased innovation, improved decision-making, enhanced efficiency, new revenue streams and improved customer experiences. Overall, sharing data can help organizations gain a competitive edge, improve their bottom line, and drive growth and innovation in their industries. While sharing data can bring economic benefits, it also carries risks for privacy and self-determination. Sharing data may violate laws and regulations governing data privacy, security, and confidentiality. Organizations need to carefully consider the risks and benefits of data sharing and take steps to mitigate these risks.

The numerous bureaucratic requirements, especially those in the Data Governance Act concerning Data Intermediation Services, are meant to increase transparency and traceability – and thus trust in services that rely on innovative data governance instruments to share data among organisations. Despite this positive effect, it remains to be seen, if they will not lead to reluctance and even disuse of newly introduced data governance instruments instead of strengthening the Digital Single Market.

Two instruments seem (despite the mentioned drawbacks) particularly promising when it comes to those data government approaches that have newly been framed by new legal requirements by the merging "data law": data cooperatives and data altruism. These approaches are covered in more detail in the "Mozilla Data Governance Playbook". We thus refer readers interested in learning more about these particular approaches to the "Playbook", which can be accessed here:

https://foundation.mozilla.org/de/research/library/is-that-even-legal/germany/

Abbreviations

AIA Artificial Intelligence Act
AufenthG Aufenthaltsgesetz
BDSG Bundesdatenschutzgesetz
BGB Bürgerliches Gesetzbuch
BGH Bundesgerichtshof
BT-Drs. Bundestags-Drucksache
BVerfGE Entscheidungen des Bundesverfassungsgerichts
cf compare
CFR Charter of Fundamental Rights of the European Union
COM Communication
CR Computer und Recht
DA Data Act
DCD Digital Content Directive
DEK Datenethikkommission
DGA Data Governance Act
DMA Digital Markets Act
DNG Datennutzungsgesetz
DSA Digital Services Act
DuD Datenschutz und Datensicherheit
e.g. exempli gratia
EC European Community
ECJ European Court of Justice
ECHR European Convention on Human Rights
Ed. Editor
Eds. Editors
eID electronic Identity
et al. and others
et seq. et sequens
EU European Union
FDP Freie Demokraten
GDPR General Data Protection Regulation
GeschGehG Gesetz zum Schutz von Geschäftsgeheimnissen
GG Grundgesetz
GWB Gesetz gegen Wettbewerbsbeschränkungen
i.e. id est
JuSchG Jugendschutzgesetz
MMR Multimedia und Recht
NFC Near Field Communication
NJW Neue Juristische Wochenschrift
para paragraph
PAuswG Personalausweisgesetz
PIMS Personal Information Management System
RDV Recht der Datenverarbeitung
RKI Robert-Koch-Institut
SPD Sozialdemokratischen Partei Deutschlands
SVR Straßenverkehrsrecht
TMG Telemediengesetz
TTDSG Telekommunikation-Telemedien-Datenschutz-Gesetz
UID unique identifier
UrhG Gesetz über Urheberrecht und verwandte Schutzrechte
Vol. Volume
ZD Zeitschrift für Datenschutz
ZD-Aktuell Newsdienst ZD-Aktuell

Literature

Blankertz, A./Specht-Riemenschneider, L., Neue Modelle ermöglichen – Regulierung für Datentreuhänder, Berlin 2021, accessible at: https://www.boell.de/sites/default/files/2021-08/bo%23776ll.brief%20G16%20Neue%20Modelle%20ermo%23776glichen.pdf.

Calliess, C./Ruffert, M. (Eds.), EUV/AEUV – Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 6th edition, München 2022 (quoted as: *Author*, in: Calliess/Ruffert 2022).

Denker, P./Graudenz, D./Schiff, L./Schulz, S. E./Hoffmann, C./Jöns, J./Jotzo, F./Goeble, T./ Hornung, G./Friederici, F./Grote, R./Radusch, I., „Eigentumsordnung" für Mobilitätsdaten – Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive, Berlin 2017, accessible at: https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile.

Dreier, T./Schulze, G. (Eds.), Urheberrechtsgesetz, 7th edition, München 2022 (quoted as: *Author*, in: Dreier/Schulze 2022).

Ensthaler, J., Industrie 4.0 und die Berechtigung an Daten, NJW 2016, 3473-3478.

Geminn, C. L., Daten für alle? – Zum Diskussionspapier der SPD, ZD-Aktuell, 06492.

Geminn, C. L./ Johannes, P. C. (Eds.), Europäisches Datenrecht, Baden Baden 2023 (in preparation).

Gersdorf, H./Paal, B. P. (Eds.), BeckOK Informations- und Medienrecht, 38. Edition, München 2021 (quoted as: *Author*, in: Gersdorf/Paal 2021).

Härting, N., „Dateneigentum" – Schutz durch Immaterialgüterrecht?, CR 2016, 646-649.

Hennemann, M./v. Ditfurth, L., Datenintermediäre und Data Governance Act, NJW 2022, 1905-1910.

Hoeren, T., Datenbesitz statt Dateneigentum – Erste Ansätze zur Neuausrichtung der Diskussion um die Zuordnung von Daten, MMR 2019, 5-8.

Jandt, S./Steidle, R. (Eds.), Datenschutz im Internet – Rechtshandbuch zu DSGVO und BDSG, Baden-Baden 2018 (quoted as: *Author*, in: Jandt/Steidle 2018).

Johannes, P. C., Europäisches Datenschutzrecht – ein Spickzettel, ZD-Aktuell 2022, 01166.

Kempny, S./Krüger, H. S./Spindler, M., Rechtliche Gestaltung von Datentreuhändern – Ein interdisziplinärer Blick auf „Data Trusts", NJW 2022, 1646-1650.

Kriesel, T., Rechtsfragen der digitalisierten Wirtschaft: Datenrechte – Eine Stellungnahme, Berlin 2019, accessible at: https://www.bitkom.org/sites/main/files/2019-09/bitkom-stellungnahme-zu-datenrechten_langfassung_final_0.pdf, quoted as: bitkom 2019).

Köhler, H./Bornkamm, J./Feddersen, J. (Eds.), Gesetz gegen den unlauteren Wettbewerb, 41st edition, München 2022 (quoted as: *Author*, in: Köhler/Bornkamm/Feddersen 2022).

Meyer, J./Hölscheidt, S. (Eds.), Charta der Grundrechte der Europäischen Union, 5th edition, Baden-Baden 2019 (quoted as: *Author*, in: Meyer/Hölscheidt 2019).

Micheli, M./Ponti, M./Suman, A. B./Craglia, M., Emerging model of data governance in the age of datafication, 2020, accessible at: https://journals.sagepub.com/doi/epub/10.1177/2053951720948087.

Michl, F., „Datenbesitz" – ein grundrechtliches Schutzgut?, NJW 2019, 2729-2733.

Müller, J. K. M., Dateneigentum in der vierten industriellen Revolution?, DuD 2019, 159-166.

Münchener Kommentar zum Lauterkeitsrecht, edited by Heermann, P. W./Schlingloff, J., Vol. 2: §§ 7-20a UWG, Geschäftsgeheimnisgesetz, 3rd edition, München 2022 (quoted as: *Author*, in: MüKoUWG 2022, Vol. 2).

Nebel, M., Alles abwählen: Mit der Einwilligungsverwaltungs-Verordnung gegen den Cookie-Banner-Dschungel, ZD-Aktuell 2022, 10321.

Peschel, C./Rockstroh, S., Big Data in der Industrie – Chancen und Risiken neuer datenbasierter Dienste, MMR 2014, 571-576.

Petri, T., Die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten, DuD 2022, 413-

Rehbinder, M./Peukert, A., Urheberrecht und verwandte Schutzrechte, 19th edition, München 2023.

Roßnagel, A., Fahrzeugdaten – wer darf über sie entscheiden?, SVR 2014, 281-287.

Roßnagel, A., Rechtsfragen eines Smart Data-Austauschs – Datengetriebene Kooperation in der Industrie, NJW 2017, 10-15.

Roßnagel, A., Datenschutz in einem informatisierten Alltag, Berlin 2007.

Roßnagel, *A.* (Ed.), Handbuch Datenschutzrecht, München 2003 (quoted as: *Author*, in: Roßnagel 2003).

Roßnagel, A./Geminn, C. L., Vertrauen in Anonymisieerung – Regulierung der Anonymisierung zur Förderung Künstlicher Intelligenz, ZD 2021, 487-490.

Roßnagel, A./Hornung, G. (Eds.), Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug, Wiesbaden 2019 (quoted as: *Author*, in: Roßnagel/Hornung 2019).

Roßnagel, A./Jandt, S./Marschall, K. (Eds.), Juristische Aspekte bei der Datenanalyse für die Industrie 4.0 – Beispiel eines Smart-Data-Austauschs in der Prozessindustrie, Vol. 2, 2nd edition, Berlin-Heidelberg 2017 (quoted as: *Author*, in: Roßnagel/Jandt/Marschall, in: Industrie 4.0, 2017, Vol. 2).

Roßnagel, A./Bile, T./Friedewald, M./Geminn, C. L./Grigorjew, O./Karboga, M./Nebel, M., National Implementation of the General Data Protection Regulation, Challenges - Approaches – Strategies, Policy Paper 2018, 1-13.

Schmitz, B./Buschuew, E., (Be-)Zahlen mit Daten: im Spannungsverhältnis zwischen Verbot mit Erlaubnisvorbehalt und Privatautonomie, MMR 2022, 171-176.

Specht-Riemenschneider, L./Blankertz, A./Sierek, P./Schneider, R./Knapp, J./Henne, T., Die Datentreuhand – Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, MMR-Beilage 2021, 25-48.

Spindler, G./Schuster, F. (Eds.), Recht der elektronischen Medien, 4th edition, München 2019 (quoted as: *Author*, in: Spindler/Schuster 2019).

Strech, D./Graf von Kielmansegg, S./Zenker, S., „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, Berlin 2020, accessible at: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf.

Sörup, T./Parvez, D., Nutzung von Microsoft Office 365 im Unternehmen – Datenschutz- und betriebsverfassungsrechtliche Fragestellungen und Gestaltungshinweise, ZD 2021, 291-297.

Taeger, J., Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018, RDV 2017, 3-9.

Völker, J. C./Schnatz, A./Breyer, J., Chancen und Risiken von Cloud-Produkten im Unternehmen – Cloud Computing – mehr als nur SaaS, MMR 2022, 427-435.

Wandtke, A.-A./Bullinger, W. (Eds.), Praxiskommentar Urheberrecht, 6th edition, München 2022 (quoted as: *Author*, in: Wandtke/Bullinger 2022).

Other Sources

Bundesministerium des Innern und für Heimat (Ed.), Datenethikkommission, Gutachten der Datenethikkommission, Berlin 2019, accessible at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.

Bundesministerium des Innern und für Heimat, Software für das Online-Ausweisen, accessible at: https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/technik/software/software-node.html.

Deutscher Bundestag – Unterabteilung Europa (Ed.), Die Anwendbarkeit von § 19a GWB im Lichte des europäischen Gesetzgebungsverfahrens zum „Digital Markets Act", Berlin 2022, accessible at: https://www.bundestag.de/resource/blob/880748/856d83cb24c61822c508aa47f27e18e7/WD-7-114-21-PE-6-067-21-pdf-data.pdf.

Deutscher Ethikrat (Ed.), Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, Berlin 2018, accessible at: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf.

Enumeration of the initial Common European data spaces, 2023, accessible at: http://dataspaces.info/common-european-data-spaces/#page-content.

European Commission (Ed.), Shaping Europe's digital future – A European Strategy for data, Brüssel 2022, accessible at: https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

Janzen, D., Das Problem von Datensilos – und wie gutes Datenmanagement sie aufbricht, in: d.velop blog, 15 October 2021, accessible at: https://www.d-velop.de/blog/digitaler-wandel/datensilo/.

Justizministerium Nordrhein-Westfalen (Ed.), Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder, Deidesheim 2017, accessible at: https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf.

Rashedi, J., Was ist ein Datensilo?, in: SpringerProfessional – Datenmanagement, 22. October 2020, accessible at: https://www.springerprofessional.de/datenmanagement/crm/was-ist-ein-datensilo-/18510004.

Robert-Koch-Institut, Datenspende gegen Corona – die Corona-Warn-App, accessible at: https://corona-datenspende.de/.

Open Definition 2.1, Open Knowledge Foundation, https://opendefinition.org/od/2.1/en/.

SPD, Bündnis 90/Die Grünen, FDP (2021): Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), 20. Legislaturperide, Berlin 2021.

What is Open Data?, Open Data Handbook, https://opendatahandbook.org/guide/en/what-is-open-data.