moz://a

Is that even legal?

A guide for builders experimenting with data governance in **Germany**

February 2023

By Christian L. Geminn, Paul C. Johannes, Johannes K. M. Müller, and Maxi Nebel

Project Group Constitutionally Compatible Technology Design (provet), University of Kassel

About Mozilla

Mozilla's mission is to ensure the internet is a global public resource, open and accessible to all. An internet that truly puts people first, where individuals can shape their own experience and are powerful, safe, and independent.

Founded as a community open source project in 1998, Mozilla currently consists of two organizations: the nonprofit Mozilla Foundation, which leads our movement building work; and its wholly owned subsidiary, the Mozilla Corporation, which leads our market-based work, including the development of the Firefox web browser. The two organizations work in close concert with each other and a global community of tens of thousands of volunteers under a single banner: Mozilla.

Acknowledgements

The authors are members of the Project Group for Constitutionally Compatible Technology Design (provet) at the Research Center for Information System Design (ITeG) at the University of Kassel. The group conducts interdisciplinary research projects on the legal issues of digitization, seeking to design digital technology in a legally compatible way and to develop the law in a technology-appropriate manner.

We would like to thank Stefan Baack, Christian Djeffal, Solana Larsen, Verena Müller, and Kasia Odrozek, who have provided valuable feedback on this work. We also thank Kristina Shu and Nancy Tran from Mozilla Foundation's design team for their support in designing this report. Ran Zheng created the illustrations you'll find throughout these pages. Thanks are further due to J. Bob Alotta, Champika Fernando, Mehan Jayasuriya, EM Lewis-Jong, Jackie Lu, Anouk Ruhaak, Udbhav Tiwari, and Richard Whitt for informing the direction of this project.

This work was led by Mozilla's Insights team. Eeva Moore led design and engagement work, Kenrya Rankin edited the research, and Neha Ravella provided project management support. Maximilian Gahntz was the project lead.

Disclaimer

The content of this report does not constitute legal advice. Please seek the advice of a qualified attorney.

Table of Contents

1. Preface

By Mozilla Insights

It's a long-established fact: today's data economy is not built on a level playing field. The people and communities whose data form its lifeblood are fighting to retain or regain control over their data and the value created from it. All too often, data is extracted and processed far removed from its source, serving the interests of the organizations that collect it rather than the people it impacts. This is why it's important to explore new ways to govern data: to shift control, strengthen agency, to share value. Through the Mozilla Foundation's Data Futures Lab and our work around data governance, we are working to challenge this current paradigm.

Reimagining, reconstituting, and rebalancing data governance requires system-level change, but opportunities to implement new ideas for better data governance often also exist within existing paradigms and legal frameworks. Just as the open source movement challenged copyright laws to introduce open licensing decades ago, builders can similarly defy existing laws and regulations to push the boundaries of how data is governed. Builders can shape new norms by leveraging opportunities present in existing rules. But to do so, they need a firm understanding of current realities. We aim to help them navigate existing legal landscapes so they can help pave the way for better data governance models and policy in the future.

The primary goal of this research is therefore twofold:

- To provide builders with an overview of the current (and changing) legal landscape governing the collection, management, sharing, and use of data in their country;
- to identify opportunities for what we call "alternative data governance" models within existing legal landscapes — specifically, where the regulatory status quo offers pathways to implement new approaches that shift power from data collectors to data subjects — that create meaningful incentives for the benefits of data to be shared between various parties and enable data to serve individual or collective interests.

The guiding question is: What can be built where, and using which levers, from a legal standpoint?

The analysis in this guide will provide builders with a map of laws and regulations relating to data and opportunities for experimentation. It will also provide concrete dos and don'ts for builders experimenting with new approaches to data governance.

1.1 Overview

In addition to providing an overview of the most important German and EU laws shaping data governance in Germany and the most relevant conceptual approaches to data governance, this report also features two case studies that explore particularly promising areas for experimentation: one on data cooperatives and another on data altruism as envisioned by the EU's Data Governance Act.

In its overview of the legal landscape, the report outlines the constitutional basis for how data must be governed in Germany in the EU, then addresses the most important legislation at both the EU and the national levels. This includes the EU's General Data Protection Regulation (GDPR) and the ePrivacy Directive and corresponding national data protection laws, as well as adjacent areas like copyright law and rules relating to trade secrets. The report also discusses legislative initiatives that are currently being implemented or negotiated in the EU, in particular the Data Governance Act, which is intended to facilitate more sharing and re-use of data in the EU.

The report also distinguishes between different approaches that are conceptual to data governance, most notably between data sovereignty and data intermediation services (DIS). The former term encompasses approaches that aim to strengthen people's agency and control over their data and data that relates to them. The latter is a term coined by the EU's Data Governance Act and it describes a new category of third-party services that establish a commercial relationship and facilitate data sharing between data subjects, data holders, and data users. Additionally, the report explains a number of other data sharing approaches, including open data and data brokerage services.

In the first case study, the report discusses data cooperatives. Under the Data Governance Act, these are considered a membership-based type of data intermediation service that collects and uses data toward a shared goal. Based on collective governance and decision-making among members, data cooperatives are meant to empower members to better exercise their rights and derive value and leverage from data relating to them. The second case study discusses data altruism. This term, too, has been codified in the Data Governance Act. It aims to create the basis for more voluntary data sharing in the EU in order to increase access to data used for public interest purposes.

1.2 How to read this guide

Throughout this report, you will find a number of recurring elements that make it easy to find exactly what you're looking for. The result is a reference that does not need to be read from cover to cover in a linear way; you can simply dip in and out of different sections as needed. The recurring elements are:

- Brief summary boxes of key themes and findings from each section.
- Case studies that dive deep into specific approaches to data governance, compete with additional resources to extend your knowledge.
- Checklists of concrete steps that may help you in your journey.

Additionally, the report contains a glossary with brief explanations of specific concepts and legal texts.

What this guide does *not* include is legal advice. It rather aims to provide a starting point in your exploration of this topic to help you ask the right questions and identify areas where bespoke advice from lawyers is necessary.

2. Overview of the legal landscape

In this section:

- Data governance in Germany is regulated by various laws, including constitutional law, at the national and European level.
- Germany's Basic Law (the Grundgesetz), following rulings by the Federal Constitutional Court, recognizes the right to informational self-determination, which requires the protection of personal data. Similarly, the EU's Charter of Fundamental Rights and the European Convention on Human Rights guarantee the right to privacy.
- Data protection law in Germany is primarily governed by the EU's General Data Protection Regulation (GDPR) and the ePrivacy Directive, which have been transposed into and amended in German national law.
- Additional provisions relevant to data governance can be found in the German Civil Code and in several laws at the national level, including those on copyright, the protection of trade secrets, and data use.
- Several European legislative initiatives that are currently being implemented or negotiated will further transform the European (and German) data governance landscape.

2.1 Constitutional framework

Data governance does not exist in a vacuum. It is subject to numerous prerequisites and requirements that prohibit some approaches to data governance concepts and strengthen or weaken others. The most fundamental guidelines for data governance are found in the fundamental rights and freedoms granted through constitutional law.

National level

The supreme value of the German constitution, the Basic Law (Grundgesetz, GG), is human dignity (Article 1(1) GG). Article 2 of the Basic Law then follows this up 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). It is an unnamed fundamental right that has been recognized since 1954. The general right to personality has since then

been used by the Federal Constitutional 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. The so-called "census decision"[1] has shaped the German approach to data governance significantly. Among other things, the Court stated that due to technological progress (in terms of collecting and combining data) there is no longer any "inconsequential data."[2] This means that even innocuous data must be treated with care, because changes in society or technology might render the data more meaningful in the future.

The right 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 a consequence of the limitation that the state must not register a human being in the entirety of their personality.[3]

While the fundamental rights enshrined in the Basic Law provide protection against actions of the state, they also mandate a proactive duty for the state to protect. In addition to this, the fundamental rights together constitute a system of values that determines the relationship between citizens. As a result, the fundamental rights form the framework for data governance both in the public and in the private sector.

The processors and controllers of data themselves can rely on Articles 12 (right to occupational freedom) and 14 (guarantee of property) GG. They have implications on both the processing of personal data and non-personal data. For data governance, this means among others things that — like any other property — data is meant to serve not only an individual or a company, but also the community as a whole.

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, "[e]veryone 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

[1] 1 Senat BVerfG, Decision on the constitutionality of the 1983 Census Act (BVerfG December 15, 1983) - BVerfGE 65, 1.
[2] BVerfG, Decision on the constitutionality of the 1983 Census Act at 45 - BVerfGE 65, 1 (45).
[3] Cf. BVerfG, Order of 16.07.1969. - BVerfGE 27, 1 (6).

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.

In summary, a cogent data governance model must:

- ☐ enable the individual data subject to control whether or not personal data is processed and the context of said processing (within the limits of other rights and interests)
- ☐ avoid the creation of huge data repositories that enable those with access to these repositories to form (or come close to) an image of the personality of individual data subjects
- ☐ enable the usage of data that serves the common good and not just individual interests
- ☐ keep in mind the differences (and similarities) between data usage by the state and by private entities, which can themselves invoke fundamental rights

2.2 Data protection law

The General Data Protection Regulation

The General Data Protection Regulation (GDPR)[4] came into effect in 2018. It states the fundamental principles relating to the processing of personal data like fairness, transparency, and data minimization.[5] The GDPR furthermore contains detailed provisions on whether and when processing of data is lawful[6] and about rights of data subjects, including the right of data access, the right to erasure, and the right to data portability. Other important provisions include the obligations and responsibilities of controllers and processors of personal data, for example concerning the security of personal data.

The ePrivacy Directive

The directive on privacy and electronic communications (ePrivacy Directive)[7] regulates privacy issues concerning telecommunication, handling of traffic data, spam, and

[4] 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.
[5] Article 5(1) GDPR.
[6] Article 6 et seqq. GDPR.
[7] 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.

cookies. As a directive, it had to be adopted into the law of the EU-member states.[8] It was amended in 2009, especially in regard to cookies — which are now subject to consent (ultimately resulting in the so-called "cookie banners") — and to spam. Besides the GDPR, it is also closely connected to directives and regulations relating to telecommunications, like the European Electronic Communications Code.[9]

The Federal Data Protection Act

Due to room left for EU member states to deviate from, specify, or amend the GDPR,[10] national data protection law remains significant. The Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) amends the European data protection law in a few key areas, for example regarding video surveillance of publicly accessible spaces, processing of "sensitive" data like health 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.

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. It transposes the ePrivacy Directive into German law, but it also contains additional provisions, like the recognition of services for managing consent and end user settings (so-called "PIMS," see below). When the ePrivacy Directive is replaced by an EU regulation, this act will also need to be overhauled.

2.3 Relevant national laws beyond data protection law

The Act on Copyright and Related Rights

The Act on Copyright and Related Rights (Gesetz über Urheberrecht und verwandte Schutzrechte, UrhG) grants authors of literary, scientific, and artistic works protection for their works. Since these can also be digital, special arrangements of data may enjoy protection via the UrhG. Investments in databases are also protected by the UrhG.

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

[8] E.g. through the German Telecommunication-Telemedia Data Protection Act
[9] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
[10] For more information refer to Roßnagel et al., "National Implementation of the GDPR."

unauthorized acquisition, use, and disclosure. It has a close link to data processing operations and systems, since insight into certain data might either directly or indirectly reveal know-how and trade secrets and therefore endanger businesses.

The Civil Code

The Civil Code (Bürgerliches Gesetzbuch, BGB) contains special private rights (Sonderprivatrechte) concerning special subject matters. Rules for all kinds of contracts, e.g. consumer contracts and rules about ownership, possession, and liability can be found in the BGB.

The Data Use Act

The act governing the use of public sector data (Data Use Act, Datennutzungsgesetz, DNG) serves the principles of open data and openness by design and by default. It is a national German law and only applies to data that is provided 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. According to the DNG, data providers are public sector bodies, universities researchers, and "other undertakings providing services of general interest."[11]

2.4 The future of European data law

Of particular importance for actors in the digital economy are 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 stages of the legislative process, are — together with the European Commission's proposition of European Data Spaces for industry, energy, and health — about to usher in a new era of European Data Law. They interlock in various ways.[12]

In the context of data governance, the DGA, the DA, and the DMA are most relevant. They will apply additionally to earlier reforms, especially the transition to the GDPR 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 toward regulation directly by the European Union. All in all, the new European Data Law will not replace established data protection law, but instead apply next to and in addition to data protection law.[13]

[11] Specifically, this refers to "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."
[12] Johannes, "Europäisches Datenrecht – ein Spickzettel."
[13] For an exhaustive introduction see (forthcoming) Geminn and Johannes, *Europäisches Datenrecht*.

The Data Governance Act

The Data Governance Act (DGA)[14] will be applicable from September 2023, with a transitional arrangement for so-called data intermediation services, which will have to comply by September 2025.[15] The DGA aims to increase trust in data sharing and to thus increase the availability of data. 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."[16]

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, and so-called "data altruism."

The Data Act

The proposed Data Act (DA)[17] aims to regulate the access to and use of data by consumers and businesses.[18] Additionally, it would regulate data holders, which are legally obliged to make data available.[19] The draft DA 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 (e.g. cloud and edge providers);
- interoperability of data processing services; and
- international data transfer.

The Digital Markets Act

The Digital Markets Act (DMA)[20] applies six months after its entry into force. The DMA contains certain obligations for so-called "gatekeepers" — providers of "gateways for a large number of business users to reach users," like search engines or video sharing

[14] 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.
[15] Cf. Articles 37 and 38 DGA.
[16] See Article 2(10) DGA.
[17] COM/2022/68 final; see also Dossier 2022/0047/COD; negotiations are ongoing; if adopted, the Data Act will probably not enter into force before 2024.
[18] Chapters II and IV.
[19] Chapter III.
[20] Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector 2022/1925.

platform services.[21] Some of these obligations are to share data with competitors and other entities. Such obligations are considered to make inadequately used data stocks more useful and at the same time provide innovation incentives for small and medium-sized enterprises (SMEs) by breaking up dominant market positions of large corporations.

[21] Recital 6(1) DMA.

3. Approaches to data governance

In this section:

- There are various approaches to conceptualizing data governance. In the context of this study, we focus on data sovereignty and so-called "data intermediation services."
- Data sovereignty primarily entails approaches that aim to strengthen people's agency and control over their data and data that relates to them. This can, for example, take the form of data portability rights or voluntary data sharing (for example through "data donations" or "data altruism").
- Data intermediation services are a new category of services introduced in the EU's Data Governance Act. These are third-party services that establish a commercial relationship and facilitate data sharing between data subjects, data holders, and data users.

With recently enacted or proposed European regulations, previous discussions on data governance have been picked up and some of the discussed approaches have been given legal standing for the first time and put on track to become widely applied. The following discusses select approaches to data governance.

3.1 Data sovereignty

Data sovereignty describes data governance approaches that are primarily aimed at increasing people's control over data. One particularly important aspect is personal data sovereignty, meaning individual control over personal data. Ensuring this 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 builders in this regard is Article 25 GDPR which stipulates data protection by design and by default.

Data as compensation

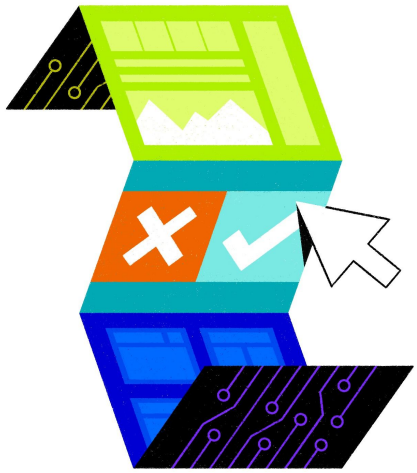
Specific rules for contracts for "digital content and digital services" have applied in German civil law since January 1, 2022. The German legislature has expanded the existing provisions in the Civil Code (BGB) on consumer contracts. Specifically, it was added that the application and principles for 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, taking into account data protection law.

No 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 themselves. 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 describes an absolute right of the individual to exclude others from handling their personal data.[22]

Nevertheless, the authority to dispose is limited, as such an absolute, unlimited power of disposition is considered incompatible with the Basic Law. The Federal Constitutional Court instead envisages a communication order.[23] The communication order does not assign exclusive rights, which has significant implications for data protection law.[24] This also holds true for the fundamental rights at the European level. As a result, there are certain uses of personal data that cannot be prohibited by the individual by claiming "ownership" of their personal data. When developing a product or service, data protection law alone forms the basis for how personal data is processed, shared, or restricted.



No absolute rights to non-personal data

Non-personal data is also of vital importance for the data economy. Naturally, this creates incentives to exclude others from the handling of this data, as would be the case with factual property. With regard to the concept of ownership under civil law, there is no absolute right in the handling of data. This ultimately leads to the conclusion that there is no such thing as data ownership of non-personal data.

[22] For ownership in personal data, see Müller, "Dateneigentum in der vierten industriellen Revolution?"
[23] Roßnagel, *Datenschutz in einem informatisierten Alltag*.
[24] Denker et al., ""Eigentumsordnung" für Mobilitätsdaten?, Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive," 46.

Prerequisite for copyright protection[25] is an "intellectual creation." Due to their automated generation in sensors or computer programs, machine data[26] or analyzed smart data[27] for instance, do not meet the requirements for an individual and unmistakable intellectual act of creation, because they lack an outstanding degree of individuality and originality. Certain efforts of investors are also protected. As a result, a database can be protected via the commercial and economic effort to create and maintain it by § 87a and following UrhG by way of a copyright.[28] Machine data and smart data analysis results can also be subject to the protection of unfair competition law, if they are confidential know-how and confidential business information (trade secrets). These are covered by the Act on the Protection of Trade Secrets.[29] For the owner, however, the trade secret does not constitute an absolute right.[30]

Data portability and interoperability

Data portability can be understood as an instrument of data governance. The GDPR's right to data portability creates a right to receive personal data relating to oneself or directly transfer one's data to another (willing) controller/service. It is recommended to provide interfaces for export and import of relevant data to facilitate the exercise of this right. This right is mostly geared toward 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).

The DMA also contains provisions regarding data portability and interoperability. For instance, gatekeepers must allow other providers as well as business users access and guarantee interoperability, so they are not disadvantaged compared to the access that the gatekeeper has.[31] Regarding end users and third parties authorized by end users — for example data cooperatives — gatekeepers will be forced to provide portability of their data.[32] Under the proposed Data Act, these rights and obligations would be expounded on by defining essential requirements regarding interoperability. The DA also seeks the development of interoperability standards for data to be reused between sectors.

[25] Copyright in the subjective sense is the creator's right to their intellectual work, cf. Hubmann, Rehbinder, and Peukert, *Urheberrecht und verwandte Schutzrechte: ein Studienbuch*, 4.
[26] Peschel and Rockstroh, "Big Data in der Industrie - Chancen und Risiken neuer datenbasierter Dienste," 572.
[27] Roßnagel, "Rechtsfragen eines Smart Data-Austauschs," 11.
[28] Wandtke and Bullinger, *Praxiskommentar Urheberrecht*, § 4 Rn. 4.
[29] This act serves to implement the Directive (EU) 2016/943.
[30] Recital 16 Directive (EU) 2016/943.
[31] Article 6(7) DMA.
[32] Article 6(9) DMA.

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." The Data Governance Act has established the term "data altruism" as a specific concept for the voluntary provision of both personal and non-personal data. Data donation can be defined as a "voluntary and informed consent that specific personal [...] data may be processed by third parties for certain purposes in a legally compliant manner as long as the processing meets the conditions attached to the donation."[33] Non-personal data can also be donated by data holders and data users alike.

Data altruism is defined in Article 2(16) DGA. It can mean two different things: 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 means "permissions of data holders to allow 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." For more details, see the case study below.

3.2 Data intermediation services

The DGA established the term "data intermediation services" (DIS) as well as a supervisory framework and an obligation to inform authorities before providing such services.[34] 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 data subjects and data holders on the one hand and data users on the other. As a result, services that establish noncommercial 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."[35]

By definition, DIS are not and may not include:

- services that transform or aggregate data for added value and for licensing purposes, but that do not establish a commercial relationship between data holders and data users;
- "services that focus on the intermediation of copyright-protected content";

[33] See Strech et al., "Datenspende," 46.
[34] Article 1(1)(b) DGA. The European Commission provides two examples for possible DIS: DAWEX and API-AGRO (see here).
[35] Recital 28(1) DGA.

- "services that are exclusively used by one data holder" or a closed group of data holders (e.g. a private data sharing pool); and
- "data sharing services offered by public sector bodies that do not aim to establish commercial relationships."[36]

The DGA names a few examples for DIS:[37]

- "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, as well as
- data pools established jointly by several legal or natural persons with the intention to license to all interested parties"; "all participants that contribute to the data pools would receive a reward for their contribution."

Data brokers, i.e. companies that purchase data from a large number of companies in order to process it and then sell it to other companies, are not regulated as data intermediation services by the DGA.[38] Service providers for the sharing of online content (according to Article 2(6) Copyright Directive[39]) that "give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users," e.g. YouTube, are also expressly excluded.[40] The same is true for closed data platforms in which 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 scope of the DGA.[41]

DIS are not limited to personal data; non-personal data may also be shared. They are generally subject to the requirement to inform authorities about their activities (Article 11 DGA) and conditions according to Article 12(a)-(o) DGA. For example, they are prohibited from using the cooperative data "for purposes other than to put them at the disposal of data users." They are monitored by the competent supervisory authorities (Article 14 DGA).

All services and data governance structures described below could — in Germany and the EU — qualify as DIS under DGA.

[36] Article 2(11) DGA.
[37] Recital 28(4) DGA.
[38] Hennemann and Ditfurth, "Datenintermediäre und Data Governance Act," 1908.
[39] 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.
[40] Recital 29 DGA.
[41] Recital 28 DGA.

Data trusts/Data fiduciaries

One broad definition of data trust or data fiduciary is: "A natural or legal person or a partnership that mediates access to data provided or held by a 'data trust' or a 'data fiduciary' in accordance with legally prescribed or contractually agreed data governance regulations (also) in the interests of third parties."[42] Data fiduciary models have in common that fiduciaries act as intermediaries for the purpose of data sharing or data access.[43] Neither the term data trust nor the term data fiduciary are defined by law.[44] They are placeholders or generic terms for various business models and ways of data sharing.

Data cooperatives

Cooperatives are rooted in the notion of solidarity and democratic decision-making. Their central principles are democratic control by the members, equal contributions, and proportional participation in the fruits of the work.[45] Existing examples of data cooperatives are purpose-driven, i.e. they pool their data to achieve specific goals that usually go beyond supporting members in the exercise of their data rights. The DGA, for the first time, defines and regulates data cooperatives as a special form of DIS whose goals are to aid its members in the exercise of rights relating to data, to make it possible to exchange views on data processing purposes and conditions among the members, and to influence the terms and conditions of data processing both within the cooperative and with regard to third parties. In summary: to strengthen the position of the individual members of the group. For more details, see Case Study #1 below.

Personal Information Management Service

Personal Information Management Service (PIMS) can be understood as a form of data trust, in the sense that they mediate access to personal data. PIMS can help the data subject exercise control over data concerning them by implementing their requirements toward data users as a service or automatically. The management function of the service then consists of the mediation of the data in the interest of the data subject to data processors with whom they negotiate access contracts, including, for example, the monetization of the data and the data subject's participation in it.

Heavily regulated under German law are PIMS regarding cookies. So-called services for the administration of consents granted under § 26 TTDSG can seek government

[42] Specht-Riemenschneider et al., "Die Datentreuhand," 25.
[43] Specht-Riemenschneider et al., 26.
[44] "Fiduciaries" and "trusts" are different legal entities, especially in common law.
[45] Knapp, Kobler, and Richter, "Was der Bauer (nicht) kennt … Datengenossenschaften," 444.

recognition.[46] § 26 TTDSG is intended to provide them with a secure and enabling legal framework.[47] However, there is no general recognition obligation for PIMS providers.

Other data intermediation services

Data marketplaces are platforms where users can buy and sell data to other users; the provider of the marketplace itself does not necessarily provide any data for sale. A data pool is commonly used for sharing data among multiple users and/or devices within one organization. Data sharing pools are commonly viewed as a solution to break open data silos. Further, DIS could function as "orchestrators of data sharing ecosystems that are open to all interested parties."[48] In order to support the free and safe international flow of data, the European Commission has proposed establishing "domain-specific common European data spaces for data sharing and data pooling."[49] Specific data sharing pools are the Common European data spaces defined by the European strategy for data.[50]

3.3 Other data sharing models

Open data

There is no legal definition of open data. Builders can use Creative Commons or other open source licenses to share data freely. These are in principle compatible with German laws on intellectual property, copyright, and related rights.

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 the obtained information. The data may be collected, for example, from public records, purchased from companies, via webtracking, or through loyalty cards. Data brokers are not considered to be DIS.[51] The German legislature inserted a provision into the BDSG specifically to protect commercial transactions in the case of scoring and credit reports.[52]

[46] PIMS according to TTDSG would be DIS according to DGA; Botta, "Delegierte Selbstbestimmung?" 949.
[47] Bundestag, "BT-Drs. 19/29839."
[48] Recital 28(4) DGA.
[49] Recital 2(7) DGA.
[50] COM/2020/66 final.
[51] Recital 28 DGA.
[52] See § 31 BDSG.

Public data trusts/re-use of data pursuant to DGA

The term "public data trust" broadly refers to a model of data governance in which a public actor accesses, aggregates, and uses data about its citizens, including data held by commercial entities, with which it establishes a relationship of trust.[53] The term is not legally defined. Public data trusts can be DIS in the sense of the DGA if they offer their services commercially.

Data trusts/fiduciaries and other services not classified as DIS

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

[53] Micheli et al., "Emerging Models of Data Governance in the Age of Datafication."

4. Case Study #1: Data cooperatives

In this section:

- Data cooperatives are a special form of data intermediation services under the EU's Data Governance Act (DGA). Data cooperatives (as defined by the DGA) are membership-based organizations collecting, sharing, and using data toward a shared goal.
- They have the potential to help members exercise their rights relating to their data; facilitate collective decision-making about what and how data is collected and used; and strengthen members' economic or bargaining position by providing collective value derived from the shared data.
- To be recognized as a data cooperative by the EU and carry the EU's "seal of approval," they need to meet several requirements specified by the DGA.

4.1 What is it?

The idea of the cooperative is based on the premise that by banding together, the interests of the members of the cooperative can be better achieved. The members of a cooperative usually contribute their respective strengths, act among themselves as equals, and in this way promote its purposes. Data cooperatives — as associations of data producers or data holders that are founded according to cooperative principles — enable self-empowerment with regard to data as a resource. A data cooperative can be set up in different ways and is as such not regulated as a single legal model.

The DGA does however make an effort to regulate data cooperatives, although only rudimentarily and with specialized main objectives. These objectives are to support their members as they exercise their data rights, to create an internal forum to negotiate fair data processing purposes and conditions, and to unify (and thus strengthen) negotiating power vis-à-vis third parties. This includes support "with regard to making informed choices before they consent to data processing."[54] These cooperatives are therefore only a subset of conceivable data cooperatives.[55] In the DGA, they exist as a special form of data intermediation service (DIS).[56] [57] Data

[54] Article 2(15) DGA.
[55] Mozilla defines data cooperative as a "legal construct to facilitate the collaborative pooling of data by individuals or organizations for the economic, social, or cultural benefit of the group."
[56] See II. b. Data Intermediation Services.
[57] See Article 10(c) DGA.

cooperatives are organizations "constituted by data subjects, one-person undertakings, or SMEs who are members" of that organization.[58]

Possible areas of application arise e.g. in manufacturing and in the service sector, such as in banking, logistics, and tourism. Another example is the use of agricultural data. Farmers have a significant interest in data from and for their relevant location in order to optimally plant, sow, fertilize, and harvest.[59] They would thus benefit from establishing a data cooperative with other farmers in the region. Last but not least, health-related data could be shared in a cooperative for medical research or clinical trials. Here, not only members, but society at large could benefit greatly.[60]

Data cooperatives can be set up in a way that each individual member of the cooperative simultaneously provides data and in return benefits from the data provided by the other members. However, they can also be operated in such a way that it is possible to be part of a data cooperative without having any interest in receiving data from other members of the cooperative. The purposes of the data usage are defined jointly within the data cooperative.

DIS and thus data cooperatives are not limited to personal data. As a result, data that has no personal references (and is thus outside the scope of data protection law) may also be shared. DIS are generally required to notify the supervisory authority (which is meant to monitor them)[61] about the intent to provide a DIS and must meet certain conditions regarding the way and means of providing DIS[62] (see below). They are exempt from these requirements if they are recognized data altruism organizations (see Case Study #2).[63]

4.2 Who is this relevant for?

Potentially every type of DIS could be established as a data cooperative between data subjects and data holders or data holders exclusively.

[58] This means that larger corporations are precluded from forming or entering into data cooperatives within the meaning of the DGA.
[59] Atik and Martens, "Competition Problems and Governance of Non-Personal Agricultural Machine Data," 391 et seq.
[60] Hafen, "Personal Data Cooperatives – A New Data Governance Framework for Data Donations and Precision Health."
[61] Article 14 DGA.
[62] Article 12(a)-(o) DGA.
[63] Article 15 DGA.

There are four primary scenarios for cooperatives of data holders:

1. to form a cooperative with competitors and rivals
2. to form a cooperative with others from the same sector that are not competitors or rivals (e.g. because they are exclusively active in other countries)
3. to form a cooperative with partners from other sectors in order to work toward a common objective
4. to form a cooperative with partners from other sectors that work toward their own objectives

Another option would be to enter into a data cooperative simply for the (direct) benefit of the other members. For example: A SME shares data with suppliers to help them develop better products or services. This might, however, yield indirect benefits for the SME in the form of better products and services that can be provided by other members of the cooperative.

The data cooperative approach is especially relevant for builders that are one-person undertakings, startups, or SMEs because of the recognition data cooperatives receive through the DGA and because it yields many advantages, such as gaining or offering access to data that would otherwise not be accessible.

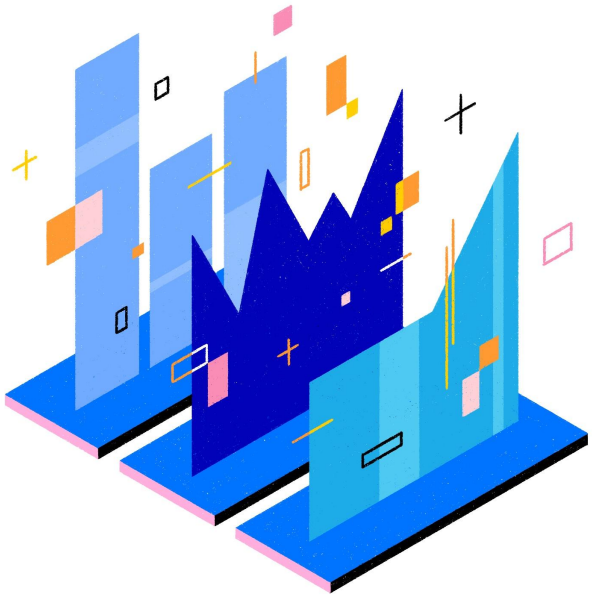
Is this the right approach for me?

- ☐ Am I unwilling to or incapable of developing my service or product without the support (regarding both access to data as well as the exercise of my rights) of a group of like-minded others?
- ☐ Do I need access to data that would otherwise be inaccessible to me?
- ☐ Do I aim at a small, but potentially more specialized scale?
- ☐ Do I seek to receive additional data in return for investing my data?
- ☐ Do I seek to join forces with like-minded builders?
- ☐ Do I want to create one voice in order to be represented against larger competitors on the market?
- ☐ Do I want to support the members of the data cooperative in the exercise of their rights with respect to certain data?

4.3 Why do this?

According to the DGA, data cooperatives have three main objectives:[64] First, they are to support their members in the exercise of their rights with respect to certain data. This includes the rights of data subjects *and* data holders, e.g. data processors. Therefore, data cooperatives could safeguard the individual rights of data subjects similar to collective bargaining as well as by asserting rights of individual data subjects or holders as their representatives. A builder could also establish a cooperative that primarily seeks to maintain and strengthen the privacy of data subjects. Such a business could be profit-oriented (for altruistic, not-for-profit activities see Case Study #2), but builders would have to keep in mind that ultimately the strengthening of data sovereignty of data subjects is one of their main objectives.

Second, data cooperatives are supposed to further the exchange of views on data processing purposes and conditions. Members of the cooperative jointly decide on the purposes and conditions of data processing. Any new member adds to the voices represented in the cooperative and may have a part in steering the cooperative. The ideal outcome would be that the cooperative best represents the interests of its members in relation to their data and beyond.



Third, data cooperatives are meant to "negotiate terms and conditions for data processing on behalf of [their] members before giving permission to the processing of non-personal data or before they consent to the processing of personal data."[65] This objective relates to an increase in outward negotiating power that individual members could not achieve on their own.

Since a lone entity would certainly have to work harder to reach its envisaged goals or would not be able to reach them at all due to the lack of access to certain data, teaming up in a group of like-minded members of a cooperative seems to be the logical answer — especially if there is competition from big players. The threshold to enter a relevant market is lowered, as is the risk of not having a sufficient input of data. The

[64] Article 2(15) DGA.
[65] Article 2(15) DGA.

builder also potentially profits from a smaller financial burden compared to purchasing data on a data market or from a data broker and therefore receives market access via a lower threshold (and "pays" with access to their own data in return). Furthermore, a data cooperative can help safeguard fair competition and business interests — not just between the members, but also with regard to any third party that wishes to access data held by the cooperative. The combined strength of the members of the cooperative is meant to lead to better terms and conditions through an increase in negotiating power.

Further, a registered DIS may benefit from the trust that is derived from regulation and oversight if it complies with the DGA. Builders will be able to use the label "data intermediation services provider recognised in the Union" in their written and spoken communication, as well as a common logo. Data subjects and others are, in terms of trust, likely to prefer cooperating with an intermediary that carries this seal of approval. Data subjects might also be more willing to consent to data processing by data cooperatives and make available personal data that otherwise could not be used.

However, certain limitations and risks remain. An intrinsic risk could lie in the openness of data cooperatives; already dominant players may seek to gain access to cooperatives as soon as they gain momentum. As a result, knowledge of data from within the cooperative may also become known to a competitor that previously excluded others and thus made it difficult for others to compete. This is counterbalanced by the fact that this dominant player would also have to make its data available to the cooperative in order to join. However, this could potentially be circumvented if a dominant player purchased a legal entity that is a member of the cooperative.

Furthermore, by joining a cooperative of data holders, a member may lose its individual advantage, if other members of a cooperative do not provide data in such a quantity or quality that it equals or surpasses their own contribution. From an economic perspective, it may however still make sense to invest data into cooperatives that are a counterweight against existing and closed data groups and where the cooperative is an option to enter a contested market. It would also be reasonable to share data in cooperatives where the members are unlikely to compete with one another (e.g., local businesses of different states; data that has a common value, but does not expose business secrets; businesses that bundle their data to receive better common output from having it analyzed by others).

Hypothetical scenario: Shopping for health insurance

In order to receive a binding estimate for a health insurance fee, a data subject would normally have to fill out a form provided by their chosen insurance company and provide highly personal and sensitive data, such as data on illnesses (their own and those that run in the family), body measures (size, weight), diet, and other (pre-)conditions that relate to their perceived health risk. To receive a personal offer, name and address would also have to be provided. An individualized and appropriate estimate can only be made if such data is provided — which potentially opens up the data to additional processing, data theft, and other risks.

A data cooperative aiming to strengthen subjects' data sovereignty in this scenario could, however, offer insurance companies new clients on the basis of anonymous estimations that are binding to the insurers. The goal would be to receive the best possible fees and insurance conditions as well as several options to choose from without transmitting sensitive personal data to numerous insurance companies. To compile the estimations, the subjects' data (which is shared via membership in the cooperative) would be processed in a safe environment, never leaving the cooperative's data spaces. A subject's data wouldn't be passed on until they chose to work with a specific insurer. The data then could be contractually restricted to be only used for the purpose of performing the contract.

Audits and other means of monitoring processing could also be part of the cooperative's requirements that a user would have to agree to, which could perhaps even include exclusive processing in the confined data space of the cooperative. An ongoing membership with the cooperative would offer the possibility to switch from one insurance provider to another with relatively little effort, if better conditions were made available elsewhere. This makes it a valuable tool for people who want to optimize both input and output when it comes to insurance. Similarly, cooperatives could be geared toward switching other types of contracts (e.g. mobile contracts or electricity).

Furthermore, the GDPR and other data protection laws still apply to any personal data processed by data cooperatives.[66] The rights of data subjects under the GDPR cannot be waived.[67] Consequently, each data subject that shares personal data has the right to transparent information, communication, and modalities for the exercise of the rights under the GDPR. "[I]t is important that the business model of such [cooperatives] ensures that there are no misaligned incentives that encourage individuals to use such

[66] Article 1(3) DGA.
[67] Recital 31(2) DGA.

services to make more data relating to them available for processing than would be in their interest."[68] "This could include advising individuals on the possible uses of their data and conducting due diligence checks on data users before allowing them to contact data subjects, in order to avoid fraudulent practices."[69] Builders would need to take this seriously when offering such services. A one-time check would not be sufficient; advising and informing correctly and fully — and monitoring data users on a regular basis — is required.

Another risk may arise from a lack of continuous monitoring and (if needed) correcting actions and provisions or other shortcomings with regard to the obligations imposed by the DGA. Rules on penalties will be established by the member states in due course and will be applicable to infringements of the notification obligations of data cooperatives pursuant to Article 11 DGA, as well as the conditions for providing DIS pursuant to Article 12 DGA. Penalties will likely be substantial[70] and be as high as penalties under the GDPR.[71] Builders that seek to establish a data cooperative or become a member of an already existing cooperative should thus first ascertain that they can meet the compliance obligations.

4.4 Where do you start?

Step 1: Legal formation

There are various ways to establish a data cooperative. The DGA does not prescribe a certain form,[72] but does require that DIS are provided via a legal person who is separate from the data holders or data subjects. In Germany, a data cooperative might therefore be set up as any kind of registered legal commercial business or cooperation, partnership with legal capacity, or registered association.[73] A cooperative of data holders could be established as a separate cooperation or registered cooperative, where data holders hold shares according to their investment. Data subjects can be owners of such a business in their own right or be a member of a cooperative. Data subjects need to be members of the organizational structure of the cooperative.[74] They

[68] Recital 30(4) DGA.
[69] Recital 30(5) DGA.
[70] Recital 55(2) DGA.
[71] See Article 83(4) and (5) GDPR.
[72] Regulation (EC) 1435/2003 established the legal form of the European Cooperative Society (Societas Cooperativa Europaea — SCE); it was created to remove the need for cooperatives to establish a subsidiary in each member state of the EU; the DGA cooperative does not have to be formed as a SCE.
[73] Despite the fact that "data cooperative" is literally translated into "Datengenossenschaft" in the German language version of the DGA and German law allows for the formation of "Genossenschaften" as legal persons (see Genossenschaftsgesetz, GenG), data cooperatives are not limited to that form in Germany.
[74] Therefore it is debatable whether a simple commercial relationship between data subject and data cooperative, like the purchase of a service, would satisfy Article 2(15) DGA.

also need to buy shares in the business or the cooperative, which is subject to a higher degree of formalism.[75] For a data cooperative whose objective is not commercial business and that seeks to gain as many data subjects as members as possible, a sensible and secure way under German law to do so would be to establish itself as a registered association.[76] PIMS[77] can be organized as data cooperatives, too. Key considerations in terms of governance are, for example, that the organization's stated purposes align with the main objectives for data cooperatives and that organization's rules and bylaws reflect these as well. A data cooperative with establishments in more than one EU member state would be under the jurisdiction of the member state where its main establishment is located.

Step 2: Notification as DIS in line with the DGA

DIS that fall into the scope of the DGA are subject to a notification procedure. This applies to data cooperatives within the meaning of the DGA as well. The notification procedure itself can be found in Article 11 DGA. A builder would first have to inform the competent authority (which will be announced by September 2023) that they intend to offer services as a data cooperative.

The notification has to include the following:

- ☐ the name of the data cooperative
- ☐ its "legal status, form, ownership structure, relevant subsidiaries and, [if applicable], registration number"
- ☐ its address
- ☐ "a public website where complete and up-to-date information on the data [cooperative] and the activities can be found"
- ☐ its contact persons and contact details
- ☐ a description of the DIS the data cooperative intends to provide[78]

[75] E.g. membership to a registered cooperative would have to be acquired through a written, unconditional declaration of accession and the admission of the accession by the cooperative, § 15 GenG.
[76] Registered Associations pursuant to § 22 BGB are legal persons and the act of joining the association can be allowed by informal declaration, e.g. by email or via a website.
[77] See II. b. 3. Personal Information Management Service (PIMS).
[78] Article 11(6) DGA.

The cooperative may commence its activities after submitting the notification. The notification entitles the cooperative to provide its services in all EU member states.

Step 3: Compliance with Article 11 and Article 12 DGA

At the request of the data cooperative, the competent authority has to confirm that the data cooperative complies with Article 11 and Article 12 DGA. The data cooperative may then use the label "data intermediation services provider recognised in the Union" as well as a common logo that all DIS recognized in the European Union share. The data cooperative also has to display the common logo clearly on every online and offline publication that relates to its data intermediation activities.

Most of these conditions also have to be met in regard to personal data, since they are governed by the GDPR. In fact, most of the conditions here have a direct counterpart for personal data via the requirements set forth in the GDPR.

Data cooperatives, as any other DIS governed by the DGA, are also monitored by the competent supervisory authorities.[79] The data cooperatives must provide all information necessary to verify compliance.

Data cooperatives have to ensure compliance with the requirements in Article 12 DGA, e.g.:

- ☐ prohibition to use the cooperative data for purposes other than to put them at the disposal of data users
- ☐ provision of services through a separate legal person
- ☐ commercial terms, including pricing, may not be dependent upon use of other services provided by the cooperative or by a related entity
- ☐ data collected about "activity of a natural or legal person for the purpose of the provision of the [DIS]" may only be used for the development of the DIS
- ☐ data shall be shared "in the format in which it [is received] from a data subject or a data holder"; it shall be converted "into specific formats only to enhance interoperability"
- ☐ Provision of a procedure for access that is "fair, transparent, and nondiscriminatory for both data subjects and data holders, as well as for data users"
- ☐ prevention of "fraudulent or abusive practices in relation to parties seeking access" to data
- ☐ appropriate provisions in the event of insolvency
- ☐ "appropriate measures to ensure interoperability with other DIS"

[79] See Article 14 DGA.

- ☐ prevention of the transfer of or access to non-personal data that is unlawful
- ☐ duty to inform data holders in event of an unauthorized transfer, access, or use of non-personal data
- ☐ ensure an appropriate level of security for the storage, processing, and transmission of non-personal data
- ☐ "ensure the highest level of security for the storage and transmission of competitively sensitive information"
- ☐ "act in the data subjects' best interest where it facilitates the exercise of their rights"
- ☐ providing "data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data"
- ☐ maintaining a "log record of the data intermediation activity"[80]

4.5 Additional resources

Baloup/Bayamlıoğlu/Benmayer et al., White Paper on the Data Governance Act, CiTiP Working Paper 2021, pp. 29 et seq. (available here).

Bietti/Etxeberria/Mannan/Wong, Data Cooperatives in Europe: A Legal and Empirical Investigation, White Paper (available here).

DatenGenossenschaft.com — A publicly funded project that aims to help SME to establish data cooperatives as registered cooperatives under German law (Genossenschaftsgesetz, GenG).

EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), Version 1.1, pp 39 et seq.

European Commission, Shaping Europe's digital future, European Data Governance Act (available here).

[80] Article 12 DGA.

5. Case Study #2: Data altruism

In this section:

- Data altruism as envisioned by the EU's Data Governance Act (DGA) is characterized by people or organizations voluntarily sharing (or making accessible) their data in a noncommercial setting in order to create data pools that can help advance the common good.
- Data altruism activities are limited to not-for-profit organizations and aim to increase the availability of data for public interest purposes.
- To be recognized as a data altruism organization by the EU and carry the EU's seal of approval — and to garner the trust of those sharing their data — an initiative needs to register and meet several requirements specified by the DGA.

5.1 What is it?

Data altruism is a special form of using data for a common cause. Since it is usually difficult to guarantee or retrace whether one's own shared data is actually processed in ways that benefit the common good, convincing people to share their (often high-quality and context-sensitive) data requires transparent and secure processing that is subject to trustworthy monitoring. The DGA's data altruism model wants to achieve this goal through a number of instruments. It is, however, just a subset of conceivable altruism models.

Under the DGA, data altruism is distinct from DIS. There is no commercial relationship established between potential data users and data is made available for altruistic purposes.[81] A central goal of data altruism is "to contribute to the emergence of sufficiently-sized data pools made available [...] to enable data analytics and machine learning, including across the Union."[82]

It can mean two different things.[83] 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). Compensation for data subjects that provide data is limited "to the costs they incur when making their data available for objectives of general interest."[84] But data altruism can *also* mean that data holders allow the use of

[81] Article 15 DGA, see also Recital 29(4) DGA.
[82] Recital 45(4) DGA. The European Commission gives three examples for possible data altruism organizations: MyData Global, Smart Citizen, and Corona-Datenspende-App (see here).
[83] See Article 2(16) DGA.
[84] Recital 45(8) DGA.

non-personal data that they hold, e.g. machine data or research data, for objectives of general interest as provided for in national law, without remuneration. They may, however, seek compensation related to the costs they incur where they make their data available.[85]

Entities that make available relevant data based on data altruism can register as "data altruism organisations recognised in the Union."[86] These must be not-for-profit entities and meet transparency requirements and offer specific safeguards to protect the rights and interests of individuals and companies who share their data. In addition, they must comply with the rulebook (to be developed by the European Commission[87]), which will outline information requirements, technical and security requirements, communication roadmaps, and recommendations on interoperability standards. The EU member states are further meant to facilitate data altruism through organizational or technical arrangements, including making available "easily usable tools for data subjects or data holders for giving consent or permission for the altruistic use of their data" and establishing national policies for data altruism.[88]

5.2 Who is this relevant for?

The DGA states that "[p]rocessing of collected data could be done by data altruism organizations for purposes which they establish themselves or, where relevant, they could allow the processing by third parties for those purposes."[89] This means that — at first glance — there is a broad area of application for data altruism. However, the instrument is ultimately limited to not-for-profit entities, which aim to carry out data altruism activities regarding the voluntary sharing of data for objectives of general interest. Defining such objectives is, however, left to the EU member states. They may include health care, combating climate change, scientific research in the general interest, and more.[90] These aims are achieved through the legal framework of the DGA

[85] See Recital 45(1) DGA.
[86] See Recital 3(12) DGA.
[87] See Article 22 DGA.
[88] Recital 45(5 et seq.) DGA; see also Recitals 46, 53, and 54 as well as Articles 16 and 21 DGA.
[89] Recital 50(2) DGA.
[90] Article 2(16) DGA; see also Recital 45(2) and (3) DGA.

and other laws, which are meant to build trust, especially by obligating transparent and supervised processing for a greater good.

Data altruism in this respect may encourage and increase the willingness to donate data. Legal requirements for not-for-profit organizations[91] can be found in the Fiscal Code. A corporation is recognized as serving public-benefit purposes "if its activity is dedicated to the altruistic advancement of the general public in material, spiritual, or moral respects."[92] This is not the case if, for example, beneficiaries are limited to members of a family, a workforce, or an enterprise; the scope must be broader. Merely allocating funds from a corporation to a public law entity is not sufficient either.[93] The Fiscal Code lists 25 areas[94] in which progress is recognized as advancement of the general public. This list is not comprehensive — other areas may be recognized as equally valid.

Is this the right approach for me?

- ☐ Do I want to use or share data for a common cause?
- ☐ Do I need access to data to support a common cause?
- ☐ Am I fine with not earning money other than being compensated for my expenses?
- ☐ Am I willing to observe all legal requirements in order to use that data?

5.3 Why do this?

The core value of data altruism as defined by the DGA lies in trustworthiness that results from strict adherence to the legal requirements set forth in the DGA. That distinguishes it from other altruistic models. It relies on the willingness of people to share their data voluntarily because they can be assured of a controlled, restricted, and supervised processing of data that is institutionalized and will offer its benefits to society as a whole.

While in principle there is a willingness to engage in data altruism, in practice this is hampered by a lack of data-sharing tools and structures. The DGA provides for such a structure and helps assure data subjects and data holders that when they share their data, it will be handled by organizations that operate based on EU values and principles. This could allow the creation of pools of data of a sufficient quantity and/or

[91] Recital 48 DGA.
[92] § 52(1)(1) Fiscal Code (Abgabenordnung, AO).
[93] § 52(1)(2) and (3) Fiscal Code.
[94] § 52(2) Fiscal Code.

quality to generate value — provided that potential contributors to the data pools are sufficiently incentivised.

Entities recognized by the EU as data altruism organizations will be able to use the common logo designed for this purpose and can choose to be included in a public register of data altruism organizations set up for information purposes by the European Commission. Builders will also be able to use the label "data altruism organisation recognised in the Union," which is meant to stand for trustworthiness and secure data processing — thus reassuring potential supporters who currently refrain from allowing their data to be processed. This standardization also has the effect of setting a de facto minimum for what is understood as data altruism. Any organization that practices data altruism but deviates from the requirements of the DGA may become suspicious in the eyes of potential data donors and thus suffer a disadvantage. It might even be accused of false advertising when using the term "data altruism" with regard to its services.

As data altruism in regard to personal data will most likely be based on the consent[95] of the data subjects, the European Commission will develop a modular consent form (meaning that it can be tailored to the needs of specific sectors and purposes) in order to fulfill the requirements of the GDPR. This European consent form will aim to allow the collection of data across member states in a uniform format, ensuring that those who share data can easily give and withdraw consent. It is also meant to give legal certainty to researchers and others wishing to use data based on data altruism. The modular approach provides flexibility: for example, slightly broader consent (in regard to the processing purposes of personal data) is likely to emerge with regard to scientific research purposes.[96] The benefit of a modular consent form provided by the European Commission is that it eliminates the need to draft new consent forms that need to be examined regarding their legality and are at risk of being deemed insufficient by a court or supervisory authority. The standardized but flexible form thus limits liability risk with regard to obtaining and managing consent.

However, if personal data is involved, the range of consent for using this data is quite limited: "Where personal data [is] provided, the European data altruism consent form shall ensure that data subjects are able to give consent to and withdraw consent from a specific data processing operation in compliance with the requirements of [the GDPR]."[97] That means that data is "collected for specified, explicit, and legitimate purposes and [may] not [be] further processed in a manner that is incompatible with

[95] Recital 50(4) DGA.
[96] See Recital 50(5) DGA: "In accordance with Regulation (EU) 2016/679, scientific research purposes could be supported by consent to certain areas of scientific research where in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects."
[97] As is pointed out by Article 25(3) DGA.

those purposes."[98] Since that consent falls within the regime of the GDPR, it can also be withdrawn at any time, rendering any further processing from that point illegal. In this regard, managing consent may prove burdensome.

Hypothetical scenario: Fighting a pandemic outbreak

At the beginning of the COVID-19 pandemic, the tracing of potential virus spreading events became an essential step in the fight against the coronavirus. Mobile data seemed to be a reliable source for tracing and counteracting such events. Builders who had sought to gather data from data subjects as a data altruism organization would have had a great impact if they were able to receive data as, for example, a donation for the altruistic objective of developing means for the timely identification of the next potential COVID-19 hot spot, using the data solely in that respect and guaranteeing data protection at the same time.

Since different kinds of pandemics may occur in the future, the hypothetical scenario of gathering relevant data of data subjects and the need for trustworthy data altruism organizations in that area is immense. This scenario could easily be applied to any kind of health research with a significant impact on a large number of people.

Furthermore, with the DGA limiting data altruism to not-for-profit-organizations, it minimizes the risk of undue influence on data subjects so as to not "nudge consumers into a choice and behavior which may not be justified depending on the circumstances" and cause "problematic consequences for those consumers who are not willing to share their data."[99]

5.4 Where do you start?

Step 1: Registration

If you decide to register your entity as a data altruism organization, there are some rather bureaucratic steps to take. Registration is not mandatory, but it is necessary to be able to use the label "data altruism organisation recognised in the Union" and the logo provided by the European Commission.

[98] Article 5(1)(b) GDPR.
[99] BEUC, "Data Governance Act Position Paper," 7.

According to Article 18 DGA, the following general requirements must be met to register:

- ☐ "carry out data altruism activities" (requiring the organization to either already carry out such activities or to state the intention to promote objectives of general interest)
- ☐ "be a legal person established pursuant to national law to meet objectives of general interest" according to the Fiscal Code
- ☐ "operate on a not-for-profit basis and be legally independent from any entity that operates on a for-profit basis"
- ☐ "carry out its data altruism activities through a structure that is functionally separate from other activities" (meaning that a dedicated legal entity is not required, however, an isolated and protected data processing environment must be established)
- ☐ comply with the rulebook that will be developed by the European Commission, which is legally binding[100]

If the entity meets these requirements, it may submit an application to appear in the public national register of recognized data altruism organizations in the member state where the main establishment is located.[101]

The entity must provide:

- ☐ name, legal status, form, registration number (if applicable), address(es)
- ☐ "statutes of entity, where appropriate"
- ☐ "entity's sources of income"
- ☐ a public website with "complete and up-to-date information on the entity and the activities"
- ☐ the "entity's contact persons and contact details"
- ☐ "objectives of general interest it intends to promote when collecting data"
- ☐ "the nature of the data that the entity intends to control or process" (for instance whether or not special categories of personal data[102] are involved)
- ☐ "documents which demonstrate that the requirements of Article 18 [DGA (see above)] are met"[103]

[100] Article 18 DGA.
[101] Article 19(1)-(3) DGA.
[102] Article 9(1) GDPR.
[103] Article 19(4) DGA.

When all necessary information is provided and all requirements are met, the competent authority evaluates the application and is obliged to register the entity in the public national register within 12 weeks of receiving the application.[104] The registration is valid in all EU member states. If any of the information changes, the entity is obliged to notify the authority within 14 days.

Step 2: Compliance with general transparency requirements

Recognized data altruism organizations are obliged to fulfill certain transparency requirements. They have to keep full and accurate records, for instance, concerning "all natural or legal persons that were given the possibility to process data held by that recognised data altruism organisation" including their contact details, as well as detailed information on the processing activities themselves.[105] Also, the data altruism organization is obliged to submit an annual activity report that includes information about its activities in general and how objectives of general interest were promoted throughout the year.[106]

Step 3: Compliance with specific requirements

Recognized data altruism organizations must also meet specific requirements specified in Article 21 DGA to safeguard rights and interests of data subjects and data holders:

Requirements under Article 21 DGA:

- **Specific transparency:** The data altruism organization must provide certain information to data subjects or data holders prior to any processing of their data in a clear and easily comprehensible manner, mainly relating to the objective(s) of general interest pursued by the organization.
- **Purpose limitation:** Data must not be used for other objectives than those of general interest for which the data subject or data holder allows the processing.
- **Marketing:** The data altruism organization must refrain from using any misleading marketing practices to solicit the provision of data.
- **Consent:** The data altruism organization must provide tools for obtaining and the easy withdrawal of consent from data subjects or permissions to process data made available by data holders.
- **Safeguards:** In the event of unauthorized transfer, access, or use of the non-personal data that the data altruism organization has shared, the organization must inform

[104] Article 19(5) DGA.
[105] Article 20(1) DGA.
[106] Article 20(2) DGA.

data holders without delay.

- **Third parties:** If the organization involves third parties for data processing that process the data outside of the European Union, it must specify the country where data use is intended to take place.

Step 4: Compliance with data security requirements

According to Article 21(4), DGA recognized data altruism organizations must take measures to ensure an appropriate level of security for the storage and processing of non-personal data that it collects. They should "adhere to all relevant technical standards, codes of conduct, and certifications at Union level."[107] Additionally, where personal data is involved, GDPR data protection requirements apply.

5.5 Additional resources

Data altruism in general:

BEUC, Data Governance Act, Position Paper, pp. 7 et seq. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-026_data_governance_act_position_paper.pdf.

Baloup/Bayamlıoğlu/Benmayer et al., White Paper on the Data Governance Act, CiTiP Working Paper 2021, pp. 37 et seq. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703.

EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), Version 1.1, pp 39 et seq.

European Commission, Data Governance Act explained, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.

Kruesz/Zopf, The Concept of Data Altruism of the draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU, European Data Protection Law Review 4/2021, 569-579.

SMEunited position paper on European Data Governance Act (COM(2020) 767 final), pp. 5 et seq. https://www.smeunited.eu/admin/storage/smeunited/210208-smeunited-pp-on-dga.pdf.

[107] Recital 23(3) DGA.

Veil, “Data Altruism: How the EU is Screwing Up a Good ilea,” Algorithm Watch, Discussion Paper #1, https://algorithmwatch.org/de/wp-content/uploads/2022/01/2022_AW_Data_Altruism_final_publish.pdf.

Vorläufige Stellungnahme der Bundesrepublik Deutschland zum Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) COM (2020) 767 final, pp. 23 et seq. https://www.bmwk.de/Redaktion/DE/Downloads/S-T/stellungnahme-bundesrepublik-deutschland-zu-daten-governance-gesetz.pdf?__blob=publicationFile&v=4.

Data donation in the context of medical research:

Robert Koch-Institut, Corona-Datenspende-App 2.0, Daten spenden und Umfragen beantworten — Ihr Beitrag gegen Corona, https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende-allgemein.html.

Strech/Graf von Kielmansegg/Zenker et al., “Datenspende” — Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, Wissenschaftliches Gutachten, erstellt für das Bundesministerium für Gesundheit, Version 1.1.

Towards European Health Data Space (TEHDAS), Presentation of a first set of data altruism definitions, use cases and findings, https://tehdas.eu/app/uploads/2021/09/tehdas-presentation-of-a-first-set-of-data-altruism-definitions-use-cases-and-findings.pdf.

6. Glossary

Bundesverfassungsgericht (BVerfG) — German Federal Constitutional Court

Bundesgerichtshof (BGH) — German Federal Court of Justice

Data — any digital representation of acts, facts, or information and any compilation of such acts, facts, or information, including in the form of sound, visual, or audiovisual recording[108]

Data Subject — the individual person (i.e. natural person) to whom personal data relates

Deutscher Bundestag Drucksache (BT-Drs.) — printed matter of the German Federal Parliament

Entscheidungen des Bundesverfassungsgerichts (BVerfGE) — collection of decisions of the German Federal Constitutional Court

Identifiable Natural Person — one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person[109]

Personal Data — any information relating to an identified or identifiable natural person (data subject)[110]

Processing — any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organizing, structuring, storing, adapting or altering, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction[111]

SME — small and medium-sized enterprise

Telemedia — term in German law; all electronic information and communication services, unless they are telecommunications services pursuant to § 3(61) of the Telecommunications Act (TKG), telecommunications-based services pursuant to § 3(63) TKG, or broadcasting pursuant to § 2 of the Interstate Broadcasting Treaty[112]

[108] Article 2(1) DGA.
[109] Article 4(1) GDPR.
[110] Article 4(1) GDPR.
[111] Article 4(2) GDPR.
[112] § 1(1) TMG.

Bibliography

Atik, Can, and Bertin Martens. “Competition Problems and Governance of Non-Personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU.” *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 12 (2021): 370

BEUC. “Data Governance Act Position Paper.” Brussels, March 29, 2021. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-026_data_governance_act_position_paper.pdf.

Botta, Jens. “Delegierte Selbstbestimmung?” *Multimedia und Recht*, no. 12 (2021): 946–51.

Bundestag. “BT-Drs. 19/29839,” May 19, 2021.

BVerfG. Order of 16.07.1969, No. 1 BvL 19/63 (BVerfG July 16, 1969).

BVerfG, 1 Senat. Decision on the constitutionality of the 1983 Census Act (BVerfG December 15, 1983).

Denker, Phillip, Dirk Graudenz, Laura Schiff, Sönke Schulz, Christian Hoffmann, Johanna Jöns, Florian Jotzo, Thilo Goeble, and Gerrit Hornung. “"Eigentumsordnung” für Mobilitätsdaten?, Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive.” 2017, n.d. https://www.uni-kassel.de/fb07/index.php?eID=dumpFile&t=f&f=4043&token=5408d0e9eac3fa0fda9271f06e5d67cc84b646e8.

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, OJ L § (1995). http://data.europa.eu/eli/dir/1995/46/oj/eng.

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, OJ L § (2002). http://data.europa.eu/eli/dir/2002/58/oj/eng.

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 (n.d.). https://eur-lex.europa.eu/eli/dir/2019/790/oj.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (2018). http://data.europa.eu/eli/dir/2018/1972/2018-12-17/eng.

Geminn, Christian, and Paul Johannes, eds. *Europäisches Datenrecht*. 1st ed. Baden-Baden: Nomos, 2023 (forthcoming).

Hafen, Ernst. “Personal Data Cooperatives — A New Data Governance Framework for Data Donations and Precision Health.” *The Ethics of Medical Data Donation*,

edited by Jenny Krutzinna and Luciano Floridi, 137:141–49. Philosophical Studies Series. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-04363-6_9.

Hennemann, Moritz, and Lukas v Ditfurth. “Datenintermediäre und Data Governance Act.” *Neue Juristische Wochenschrift*, no. 27 (2022): 1905–10.

Hubmann, Heinrich, Manfred Rehbinder, and Alexander Peukert. *Urheberrecht und verwandte Schutzrechte: ein Studienbuch*. 18., Vollständig neu bearbeitete Auflage, 2018. Juristische Kurz-Lehrbücher. München: C.H. Beck, 2018.

Johannes, Paul. “Europäisches Datenrecht – ein Spickzettel.” *Newsdienst ZD-Aktuell*, no. 8 (2022): 01166.

Knapp, Jakob, Jonas Kobler, and Phillip Richter. “Was der Bauer (nicht) kennt … Datengenossenschaften.” In *Daten, Plattformen und KI als Dreiklang unserer Zeit*, edited by Christian Heinze and Deutsche Stiftung für Recht und Informatik, 443–58. Edewecht: OlWIR, Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2022.

Micheli, Marina, Marisa Ponti, Max Craglia, and Anna Berti Suman. “Emerging Models of Data Governance in the Age of Datafication.” *Big Data & Society* 7, no. 2 (July 2020): 205395172094808. https://doi.org/10.1177/2053951720948087.

Müller, Johannes Karl Martin. “Dateneigentum in der vierten industriellen Revolution?” *Datenschutz und Datensicherheit - DuD* 43, no. 3 (March 2019): 159–66. https://doi.org/10.1007/s11623-019-1084-8.

Peschel, Christopher, and Sebastian Rockstroh. “Big Data in der Industrie - Chancen und Risiken neuer datenbasierter Dienste.” *Multimedia und Recht Zeitschrift für Informations-, Telekommunikations- und Medienrecht*, no. 9 (2014): 571–76.

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, 119 OJ L § (2016). http://data.europa.eu/eli/reg/2016/679/oj/eng.

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, 152 OJ L § (2022). http://data.europa.eu/eli/reg/2022/868/oj/eng.

Roßnagel, Alexander. *Datenschutz in einem informatisierten Alltag*. Medien- und Technologiepolitik. Berlin: Friedrich-Ebert-Stiftung, 2007.

Roßnagel, Alexander. “Rechtsfragen eines Smart Data-Austauschs.” *Neue Juristische Wochenschrift*, no. 1 (2017): 10–15.

Roßnagel, Alexander, Tamer Bile, Michael Friedewald, Christian Geminn, Olga Grigorjew, Murat Karaboga, and Maxi Nebel. “National Implementation of the GDPR.” Karlsruhe: Forum Privatheit, 2018. https://www.forum-privatheit.de/download/national-implementation-of-the-gdpr-2018/.

Specht-Riemenschneider, Louisa, Aline Blankertz, Pascal Sierek, Ruben Schneider,

Jakob Knapp, and Theresa Henne. “Die Datentreuhand.” *Multimedia und Recht-Beilage*, no. 6 (2021): 25–48.

Strech, Daniel, Sebastian Graf von Kielmansegg, Sven Zenker, Michael Krawczak, and Sebastian Semler. “Datenspende.” Berlin: BMG, March 30, 2020. https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf.

Wandtke, Artur-Axel, and Winfried Bullinger, eds. *Praxiskommentar Urheberrecht: UrhG, UrhDaG, VGG, InsO, UKlaG, KUG, EVtr, InfoSoc-RL, Portabilitäts-VO*. 6., neu Bearbeitete und erweiterte Auflage. München: C.H. Beck, 2022.