July 2021 · Aline Blankertz & Louisa Specht

What regulation for data trusts should look like

Stiftung Neue Verantwortung

Think Tank at the Intersection of Technology and Society

Executive Summary

Data trusts are a promising concept for enabling data use while maintaining data privacy. Data trusts can pursue many goals, such as increasing the participation of consumers or other data subjects, putting data protection into practice more effectively, or strengthening data sharing along the value chain. They have the potential to become an alternative model to the large platforms, which are accused of accumulating data power and using it primarily for their own purposes rather than for the benefit of their users. To fulfill these hopes, data trusts must be trustworthy so that their users understand and trust that data is being used in their interest.

It is an important step that policymakers have recognized the potential of data trusts. This should be followed by measures that address specific risks and thus promote trust in the services. Currently, the political approach is to subject all forms of data trusts to the same rules through "one size fits all" regulation. This is the case, for example, with the Data Governance Act (DGA), which gives data trusts little leeway to evolve in the marketplace.

To encourage the development of data trusts, it makes sense to broadly define them as all organizations that manage data on behalf of others while adhering to a legal framework (including competition, trade secrets, and privacy). Which additional rules are necessary to ensure trustworthiness should be decided depending on the use case. The risk of a use case should be considered as well as the need for incentives to act as a data trust.

Risk factors can be identified across sectors; in particular, centralized or decentralized data storage and voluntary or mandatory use of data trusts are among them. The business model is not a main risk factor. Although many regulatory proposals call for strict neutrality, several data trusts without strict neutrality appear trustworthy in terms of monetization or vertical integration. At the same time, it is unclear what incentives exist for developing strictly neutral data trusts. Neutrality requirements that go beyond what is necessary make it less likely that desired alternative models will develop and take hold.

Four use cases (medical data, PIMS, product passports, and agricultural data) illustrate how risk- and incentive-based regulation might look. The goals, whether data is personal, how risky the data sharing is, and the extent to which data is shared differ among these use cases.

The first use case is **medical data,** which holds enormous potential for medical research to develop new and more personalized forms of diagnosis and treatment. At the same time, the data is highly sensitive and includes current treatment data as

well as potential future risk factors. Risks associated with sharing that data include self-censoring behavior, discrimination, and treatment failure if data is not interpreted carefully.

To use medical data more extensively, a legal basis should be created for data processing by scientific and commercial organizations for medical research with data provided by a data trust. To ensure that risks remain manageable, IT security must be certified by a state-supervised body. Furthermore, data access should be designed in such a way that only the data necessary for the research is accessible, and personal identification is reduced as much as possible, for example, with pseudonymization. Organizations that operate in areas that are likely to discriminate, such as insurance and advertising, should be excluded.

The second use case is personal information management systems (**PIMS**), which are intended to help consumers enforce their rights and interests more effectively. However, consumers have been reluctant to use these services, and companies such as large platforms have found it easy to circumvent these systems. At the same time, there is a risk of abuse in direct dealings with consumers (e.g., through misleading information and menu navigation).

To control the risks and at the same time, support the development of PIMS, we propose to make model terms and conditions for PIMS the basis for certification that identifies them as trustworthy. These terms and conditions should include minimum standards for IT security and provide explicit consent for monetization of personal data. Furthermore, there should be transparency requirements that make the monetary and non-monetary transfer of data visible. The terms and services should also contain restrictions on the use of data by affiliated services such that it takes place under the same conditions as for external services. Overall, the intention is to align PIMS with the interests of consumers. Companies such as social media platforms can then be obligated to cooperate with certified PIMS. With these safeguards, it also makes sense to allow PIMS to represent consumers more comprehensively, for example, to grant or deny consent on behalf of their users, as “authorized agents” under the California Consumer Protection Act (CCPA) do.

The third use case is **product passports,** which allow products and product attributes to be tracked across the value chain and have enormous potential for promoting a circular economy. Several initiatives promote data-based resource reuse and recycling, but they often fail due to high administrative and financial burdens and limited management relevance.

It is not obvious that there is a need for restrictive regulation of data trusts seeking to offer product passports. Instead, it is more promising to provide legal clarity on

data sharing between companies and to use government demand strategically to encourage the use of product passports in government procurement.

The fourth use case is **agricultural data,** which can help not only increase agricultural yields but also target resources more effectively. This data is increasingly being collected and used, although a major obstacle lies in the sometimes hesitant interest in digitizing farms.

Regulatory restriction of agricultural data trusts does not appear to be necessary. Instead, more incentives can be provided, for example, by making more government data available for use in the agricultural sector.

Recommendations for action across sectors

Regulating data trusts should not increase existing legal uncertainty and complexity but reduce it. This is necessary to incentivize the development of new models and approaches. Additional requirements to establish trust and reduce risks also justify lowering hurdles. Overly strict neutrality requirements inevitably mean that data trusts can be provided only by the government, which creates other potential problems. Instead, it is more productive to use legal restrictions to prevent specific conflicts of interest.

If specified requirements are met, certification can make data trusts transparent, particularly when the risk of overly restrictive regulation is high, and information asymmetries, for example, call for intervention. Another pragmatic way to promote data trusts is to use pilot projects and government demand strategically. However, this method is no substitute for developing new models, especially business models.

Whether data trusts can fulfill the high hopes placed on them depends largely on how the regulatory framework that applies to them is designed. Overall, regulatory proposals for data trusts should aim to make data use and data protection more compatible. To this end, it is helpful to focus on specific risks that are not covered by the existing legal framework; at the same time, it is also helpful to remove hurdles that stand in the way of this goal.

Table of Contens

1. Introduction

Data trusts are a promising concept for enabling the use of data while protecting it. This is the view of policymakers, business, and civil society.[1] Data trusts have the potential to become an alternative model to the large platforms, which are accused of accumulating data power and using it primarily for their own interest rather than for the benefit of their users.

For data trusts to realize this potential, they must be perceived as trustworthy. The current political strategy is to ensure trust through new regulation that goes beyond the existing legal framework. The Data Governance Act (DGA), for example, imposes the same requirements on all data services.

However, such "one size fits all" regulation risks preventing data trusts from developing in the first place, because they have to comply with rules that do not consider the potential and risks of their use cases. Yet the range of applications in which data intermediaries can offer benefits is diverse, from personal information management systems (PIMS)/consent assistants,[2] the healthcare context,[3] and research data centers[4] to data hubs for connected cars.[5]

Instead of treating these scenarios the same way, risk-based regulation should ensure security and trustworthiness for each scenario while enabling and incentivizing innovation. Rigid regulation does not ensure secure data trusts but can hamper their development in the first place. Therefore, when regulation is designed, the different functions of and challenges for data trusts should be considered depending on the use case.

In this paper, we develop an approach that systematizes the risk posed by different forms of data trusts across sectors. In four use cases, we flesh out the different

1 Translated from German "Datentreuhand". "Datentreuhand" and "data trust" are not fully equivalent; other common translations of "Datentreuhand" include "data trust" and "data steward". We define the term with reference to its German usage in section 2 and emphasize that we do not seek to designate a "Datentreuhand" with reference to UK trust law. "Data trust" in this paper also is to be understood more broadly than the consumer data trusts developed in Blankertz (2020), "Designing Data Trusts."

2 PIMS are services that can help manage and/or access personal data, see Section 4.2. and Schwartmann , Hanloser, Weiß (2021), "PIMS in the TTDSG – Proposal for regulating consent management services in the Telecommunications Telemedia Data Protection Act", March.

3 German Data Ethics Commission (2019), "Expert Opinion of the Data Ethics Commission"; German Federal Government (2021), "Data Strategy of the Federal Government", Section 2.3, January; German Council for Information Infrastructures (2021), "Workshop Report of the Data Trustship WG – Data Trusts: Potentials, Expectations, Implementation."

4 See, inter alia, Federal Government (2021), op. cit.

5 See, among others, Kerber (2018), "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data," JIPITEC 9 (3), pp. 310-331 and Gesamtverband der deutschen Versicherungswirtschaft (2018), "Datenkranz beim automatisierten Fahren gemäß § 63a StVG – externe Speicherung bei einem Datentreuhänder," position paper, August.

regulatory approaches that address risks while enabling innovation and lowering barriers to entry. In Section 2, to narrow down the models and corresponding regulation, we formulate minimum requirements for a data trust, which serves as a definition. In Section 3, we demonstrate how regulatory proposals limit the scope of data trust models and what factors should determine regulatory stringency. In Section 4, we explore the potential scope and regulatory needs of four use cases: medical data, PIMS, product passports, and agricultural data. In Section 5, we present our conclusions.

2. Definition

There is no generally accepted definition of what characterizes a data trust. The term data trust is currently used for a broad spectrum of approaches. Using the term broadly is useful if the underlying objective is to create new or alternative models. Therefore, in the following, we develop a basic definition for data trusts that encompasses these uses.[6]

To determine what constitutes data trusts, their goals are a useful starting point. An interdisciplinary exchange identified the following goals, which may or may not be combined[7]:

- *"Strengthening, guaranteeing or restoring individual or collective control over data by strengthening the position of data subjects, consumers or affected parties in terms of data protection law (e.g. by reducing information asymmetries/negotiation imbalances).*
- *Promoting the participation of data subjects (such as consumers) in the economic exploitation of data.*
- *Promoting data sharing and making data widely or selectively available to foster innovation and competition through wider data use*
- *Possibility to proactively define the conditions of data sharing*
- *Compliance with data protection regulations, e.g. through pseudonymization or encryption of personal data*
- *Preparation and provision of high-quality, pseudonymized data for science and research*
- *Data management with impartiality, transparency and undivided loyalty*
- *Prevention of unauthorized data access*
- *Restricting the dominant position of large platform operators*
- *Promoting trustworthy European platform offerings*
- *Position as an anchor of trust or intermediary between data providers and data users."*

From these objectives, three basic characteristics of a data trust can be derived:

- (also) data intermediation: A data trust incorporates a data management, transmission, and/or processing function for the benefit of another party (or parties).
- compliance with legal requirements: A data trust is bound by an existing legal framework. This means that the data trust's activities fulfill general legal requirements (e.g., data protection, antitrust law) and specific agreements in the form of a contract between the parties involved.

6 This definition is broader than the "optimal" version of consumer data trusts as a collective negotiating body developed in Blankertz (2020), op. cit.

7 _Blankertz, von Braunmühl, Kuzev, Richter, Richter, Schallbruch (2020), "Datentreuhandmodelle", available at: https://www.ip.mpg.de/de/publikationen/details/datentreuhandmodelle-themenpapier.html, own translation.

- application-dependent trust requirements: Depending on the area of application of a data trust, different mechanisms may be useful and required to achieve trust and a desirable distribution of the value derived from data. Due to the variety of possible goals, these requirements are not to be determined in general, but depend on use cases.

In the remainder, we focus on the third point. Specific requirements, possibly anchored in regulation, to be imposed on data trusts should not be based on a general ideal image of possible data intermediaries. Requirements should be chosen to achieve the most effective goals possible and exclude actual risks.[8]

8 From a legal perspective, data trusts have little to do with what is understood by the term "Treuhand" under civil law. As there are usually no absolute rights to data (see Specht, Kerber (2017), "Datenrechte – eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA", Abida-Gutachten, available at: https://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf), these cannot be transferred comprehensively. Understood differently from a non-genuine power of attorney trust, no absolute right to data is required to authorize a data trust, for example, to make an access decision for the data recipient (such as consumers or companies). If, according to recent literature, all legal relationships whose objective is internal representation of the interests of one contracting party vis-à-vis the other are included as trusts, data trusts can also be included under this concept of trusts in the broader sense. This broad understanding of trust, in turn, is not necessarily identical to the understanding of trust in other legal systems, for example, the English trust. On the similarities and differences between the trust and the trust, cf. Graf von Bernstorff (2011), "Einführung in das englische Recht", 4th ed., p. 144 f.

3. Cross-sector regulation

For stricter regulation of data services in general and data trusts specifically, various proposals have been suggested. First, we summarize and assess existing regulatory efforts (Section 3.1.). The current proposals primarily aim at imposing additional requirements on data services. Then, we develop a proposal for risk-based regulation (Section 3.2.). In this proposal, the (de)centrality of data storage and the voluntary/mandatory nature of the use of data trust models play an important role in assessing how strict regulation should be. At the same time, we take a critical look at the extent to which a neutral business model should be prescribed.

3.1. Weaknesses of current regulatory proposals

Content of the proposals

Various projects aim to regulate data trusts. The DGA is the most comprehensive, but there are several other efforts to establish additional requirements for data intermediaries.

The **Data Ethics Commission** has demanded that the federal government develop quality standards as well as a certification and monitoring system for data trusts, especially PIMS.[9] The commission mentions charitable foundations or companies as possible agents, but the latter only "if the operator earns money from the administration and not from the use of the data."[10] As explained in Section 3.2., in practice this distinction is less clear than it first appears.

The **Federation of German Consumer Organizations** (vzbv) also has demanded that PIMS act in a legally secured manner "independently, neutrally and without any economic self-interest in the exploitation of the data managed on behalf of consumers."[11] Moreover, vzbv suggests high transparency and appropriate terms and conditions. vzbv prefers foundations as an organizational form and considers remuneration of data subjects problematic.[12]

The **SPD**'s election manifesto promises the establishment of public data trusts alongside a "trustworthy data-sharing infrastructure" and an obligation for large

9 Data Ethics Commission (2020), op. cit.
10 Ibid., p. 134.
11 vzbv (2020), "Personal Information Management Systems (PIMS): Opportunities, Risks and Requirements", February, p. 11.
12 Ibid.

corporations to "share their data for public benefit."[13] The manifesto does not specify the purpose of public data trusts further. The other political parties have not published programs or are silent about the regulation of data trusts.

The **TTDSG** (Act on the Regulation of Data Protection and Privacy in Telecommunications and Telemedia) stipulates that consent management services must not have an interest in consumers giving consent or be associated with a company interested in their consent.[14] Furthermore, the TTDSG does not prescribe a specific organizational form but names "institutions organized by companies as an independent foundation, which offer so-called single sign-on solutions for the companies associated in the foundation, through which users can organize their consent" as examples.[15] Such organizations do not exist,[16] and it is not clear what incentive there is to create them.

The DGA, which was presented in draft form at the end of 2020, also imposes a number of requirements on data trusts:

- **Notification** (Art. 10): All so-called "data sharing service providers," which include data trusts, must be notified and are supervised by an authority with regard to compliance with the requirements contained in Art. 9–13 (Chapter 3).
- **Neutrality obligation** (Art. 11 No. 1–3): The provision, mediation, and use of data must be institutionally separated. Data-sharing service providers may only mediate the data and not use it for their own purposes. This also applies to the metadata, which may be used only for the development of the service. A separate legal entity is required to provide the sharing services, as well as to offer the service in a non-discriminatory, fair, and transparent manner.[17] This separation is to prevent (over)use of the data for the providers' own purposes and preferential treatment of integrated services. The stipulation possibly reflects the negative experience with the data practices of large platforms, for example, Amazon vis-à-vis Marketplace providers.[18]
- **Best interest** (Art. 11 No. 10): Where data-sharing services are offered to the data subject, the service shall act in the best interest of the data subject and facilitate the exercise of the right by advising them on the purposes of the data processing and the conditions attached.

13 SPD (2021): "Das Zukunftsprogramm der SPD", available at: https://www.spd.de/fileadmin/Dokumente/Beschluesse/Programm/SPD-Zukunftsprogramm.pdf, p. 15.

14 German Bundestag (2021), "Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Energie zu dem Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien", Drucksache 19/29839, available at: https://dip21.bundestag.de/dip21/btd/19/298/1929839.pdf

15 Ibid., p. 78.

16 One exception is netID Foundation, which was founded by Mediengruppe RTL Deutschland, ProSiebenSat.1 and United Internet and associates, and many other media and other companies. It is unclear to what extent it meets the requirement of not having an interest in consent, because the associated companies pursue different forms of data processing. More information at: https://enid.foundation/

17 Kerber (2021), "DGA – some remarks from an economic perspective", available at: https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/pdf-dateien/kerber_dga_einige-bemerkungen_21012021.pdf

18 See European Commission (2020d), Case AT.40462 Amazon Marketplace.

In addition, the DGA highlights that data-sharing services should have processes in place to prevent fraudulent or abusive behavior in relation to data access (Art. 11 No. 5), prevent illegal access or transfer of non-personal data (Art. 11 No. 7), ensure a high level of security for non-personal data (Art. 11 No. 8), and comply with competition law (Art. 11 No. 9). If this obligation means that services must comply with the established legal framework, then it is prescribed by existing laws. If this obligation means that services would further have to ensure the lawfulness of the conduct of their contractual partners, this clause would result in many new obligations for data services.

These requirements do not apply to non-profit bodies whose activity consists exclusively of collecting data for general interest provided by natural or legal persons in the form of data altruism, i.e. non-monetary sharing of data with certain non-profit organizations.

Evaluation of the proposals

The regulatory proposals impose additional requirements and hurdles for data trusts to ensure their trustworthiness. These requirements prescribe an “optimal” data model that excludes to the largest possible extent risks of data sharing. The requirements, thus, also exclude other models that may not be completely risk-free but are still desirable because their benefits may outweigh their risks.

The idealization of a completely neutral and non-profit data trust fails to recognize that regulation does not provide or create any incentives to establish such organizations. If a data trust is prohibited from pursuing its own interests as a matter of principle, it is unclear why a data trust should be set up in the first place. It makes sense to minimize potential conflicts of interest of a data trust, but there are less intrusive measures to do so than to exclude all potential interests (we develop these measures for specific applications in Section 4).

In addition, the requirements in the regulatory proposals often collide with the reality of existing “new” models: The requirement of neutrality, as described in the DGA, for example, prevents models where internal data is opened up to external parties and then further developed into a platform that incorporates data flows from third parties. Linking data services with production activities in the same company is a form of vertical integration.

There are various examples of such vertical integration. This was the case, for example, at Tony's Chocolonely, a Dutch chocolate manufacturer, which opened its Open Chain platform for tracking fairly produced cocoa for use by other chocolate manu-

facturers.[19] Similarly, the merger of the car-sharing platforms DriveNow and Car2Go created an open platform for mobility services (ordered for competitive reasons) that can be used by other providers despite vertical integration.[20] Internet of Things (IoT) platforms also often initially belong to one manufacturer (e.g., MindSphere to Siemens,[21] Home Connect Plus to Bosch[22]) before they open up to other providers.

In the context of personal data, data protection law comprehensively specifies the purposes and (strict) standards of data processing. Why additional and stricter requirements should be imposed on data trusts is not immediately comprehensible, at least if the intention is to provide incentives for the development of certain data trust models. Each additional regulatory requirement makes data trust models less feasible and less competitive compared to the direct data exchange models with which data trusts compete in the market. There is a risk that the market for intermediary services will decline or even disappear altogether because of over-regulation.[23] In summary, with an overly narrow idea of desirable data services, the current regulatory proposals risk making the development of data trusts more difficult, because they are supposed to fulfill considerable additional requirements in addition to existing legal requirements. In this way, the proposals effectively prevent abuse, but as an undesirable side effect also prevent possible beneficial forms of data exchange.

3.2. Benefits of a risk-based approach

The strictness with which data trusts are regulated should be commensurate with their risks: The riskier a data trust's activities, the stricter the rules it should be subject to. The European Commission's proposal for regulation of artificial intelligence (AI) follows the same approach.[24] Any regulatory intervention should always be linked to a need for regulation, which can result, for example, from the state's protection duties. Where the rights and interests of the persons involved face high risk, there is, in principle, a greater need for regulation than where the risks are low from the outset.[25]

19 See “Tony's Open Chain”, available at: https://www.tonysopenchain.com/
20 European Commission (2018), Case M.8744 -DAIMLER / BMW / CAR SHARING JV, 7 November.
21 https://siemens.mindsphere.io
22 https://www.home-connect-plus.com/de/app/
23 Kerber (2021), op. cit.
24 European Commission (2021), “Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence”, available at: https://ec.europa.eu/newsroom/dae/redirection/document/75788
25 Specht-Riemenschneider, Blankertz, Sierek, Schneider, Knapp, Henne (2021), “Datentreuhand: Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle”, Supplement in MMR, June

The risks of a data trust are mainly related to the rights and interests of the possible parties involved and include the following:

- the right to informational self-determination,
- the protection of business secrets,
- the protection of intellectual property and copyrights,
- freedom of occupation, freedom of research, and
- private autonomy, which is also guaranteed by fundamental rights.

These rights and interests are influenced by two overarching design parameters present in every data trust solution: The first parameter is whether use of the data trust is mandatory, and therefore, for example, data subjects must have their data

	Voluntary use	**Mandatory use**
Decentralized data storage	voluntary & decentralized e.g. certain PIMS	mandatory & decentralized e.g. gateway (AUS)
Central data storage	voluntary & central e.g. certain PIMS	mandatory & decentral e.g. car data

Figure 1: Risk-based differentiation of data trust models

Source: Stiftung Neue Verantwortung based on Specht-Riemenschneider et al. (2021)

managed by a data trust. The second parameter is whether the data is stored in a central or decentralized form, for example, in a central database or with the individual parties. These parameters differentiate the four models shown in Figure 1.

There are examples of all models. PIMS (see Section 4.2.) can be centralized or decentralized, and their use is voluntary for all parties. The gateway for the Australian energy sector is a data access point that companies must use to be granted access to data that is decentralized (see later in this section). For car data, it is possible that a centralized and mandatory approach will be imposed.[26]

Another risk factor is the processing of personal data by the data trust. This risk is comprehensively covered by data protection law, in particular the General Data Protection Regulation (GDPR), the Federal Data Protection Act (Bundesdatenschutzgesetz), and the data protection laws of the federal states (Länder), as well as special regulations such as in the Tenth Social Code (Zehntes Sozialgesetzbuch). Therefore, this paper distinguishes only between personal and non-personal use cases (see Section 4).

26 See German Insurance Association (2018), op. cit.

Risk factor: central storage of data with the data trust or decentralized storage with the data processor/affected party

A key differentiator of data trust models is where the data is stored. The data can be held centrally by the data trust or decentralized by the data processor(s) or the data subject(s).[27] As shown in Table 1, central data storage is associated with higher risks. Although it enables additional forms of data use, centralization places higher demands on the underlying infrastructure.

Table 1: Characteristics of centralized and decentralized data trust models

	Central	Decentralized
Options		
Data trust activities	Comprehensive, from access management to analysis on behalf of third parties	Limited to access management
Possible data use	Comprehensive, including exploratory data analysis	Limited to, for example, algorithm training
Infrastructure requirements	Potentially lower (e.g., if no real-time data transmission necessary)	Full integration via data trust necessary
Risks		
Control with data suppliers	Lower	Potentially higher, depending on implementation
Data protection risk	Higher	Lower
Risk of abuse by data trust	Higher	Lower
Security risk	Higher	Lower

Source: Stiftung Neue Verantwortung

Central storage at the data trust promises it can more easily manage the data. More comprehensive activities are possible, such as excluding the data processor from access (see Microsoft Cloud[28]). In the case of central storage, the data trust can

27 Cf. with similar consideration of the data trust Wendehorst, Schwamberger, Grinzinger (2020), "Datentreuhand -wie hilfreich sind sachenrechtliche Konzepte?", in Pertot (ed.), Rechte an Daten, [pp. 103-121] p. 107; Specht-Riemenschneider et al. (2021).

28 This was the concept of a collaboration between Microsoft and Deutsche Telekom, in which Deutsche Telekom was to act as a data trust for Microsoft cloud services. However, the project was discontinued in 2019; see Nitschke (2018), "Microsoft to Provide its Cloud Services From New Data Centres In Germany From 2019 In Response to Changing Customer Requirements", available at: https://news.microsoft.com/de-de/microsoft-cloud-2019-rechenzentren-deutschland/

make extensive use of the data (e.g., analyze it) or make changes (e.g., delete it). Currently, data protection law decides to what extent this is permissible. If a data trust anonymizes or pseudonymizes data, data can be held in decentralized storage, and a data trust be a central access point to grant access to anonymized or pseudonymized data to (contractually defined) third parties.

If the data trust stores the data centrally, the risks tend to be higher. The data trust has at least partial control over the data, which requires more safeguards for the data providers. Data protection, where personal data is involved, is also more difficult to ensure when data is shared directly and unencrypted with a data trust. In addition, the data trust can gain "data power" through pooling large amounts of data, which carries the risk of misuse (e.g., that insights gained in this way are not used to the advantage of the data providers). The security risk is also greater with centrally held data, as the potential damage is higher in the event of attacks against the intermediary.

Examples of data intermediaries that use different forms of (de-)centralized data storage are described below. Occasionally, centralized elements are combined with decentralized elements.

The Bundesbank's Research Data and Service Centre (FDSZ) manages access to comprehensive data sets, which include sensitive microdata. The data is held centrally at the Bundesbank and can be partially accessed. If researchers or analysts need access to granular data that falls under data protection law, they can obtain the data on-site, in which case "[t]he FDSZ ensures that only anonymized results leave the secure environment of the visiting researcher's workstation at the FDSZ."[29] Thus, security and data protection are ensured through strong restrictions on access.

In Australia, the Australian Consumer and Competition Commission (ACCC) is developing the Consumer Data Right, initially in the energy sector. Although consumers are supposed to be provided with better access to data and easier switching possibilities between suppliers, the ACCC rejected efforts for data records to be held in central storage in the energy sector.[30] Instead, a model of decentralized storage combined with a coordinating point for forwarding and passing through data, the gateway, has been adopted.[31] Figure 2 shows how the gateway plays a coordinating role without aggregating data.

29 Deutsche Bundesbank, "Research Data and Service Centre (FDSZ)", available at: https://www.bundesbank.de/de/bundesbank/forschung/fdsz/forschungsdaten-und-servicezentrum-fdsz--604430

30 Advantages and disadvantages of data access design options in the Australian energy sector were collected during a public consultation and tabulated by the ACCC in the following document; see ACCC (2019), "Consumer Data Right in Energy – Position Paper: data access model for energy data", available at: https://www.accc.gov.au/system/files/ACCC%20-%20CDR%20-%20energy%20-%20data%20access%20models%20position%20paper%20-%20August%202019.pdf

31 For a discussion of the gateway in the energy sector, see ACCC (2020), "Energy Rules Framework – Consultation Paper", p.36 f., available at: https://www.accc.gov.au/system/files/CDR%20-%20Energy%20rules%20framework%20consultation%20paper%20-%20July%202020_0.pdf

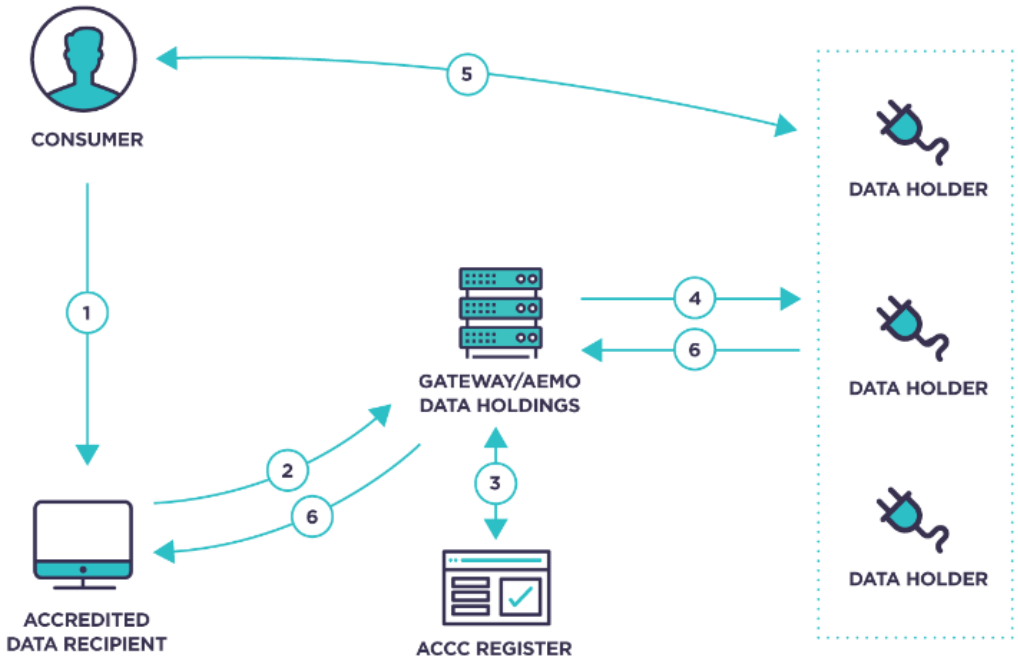

Figure 2: Overview of data flows via a gateway in the Australian energy sector

Source: ACCC (2019), 'Consumer Data Right in Energy – Position Paper: data access model for energy data', p. 14.

1. The consumer consents to an ADR obtaining their data.
2. The ADR contacts the gateway, seeking to access the consumer's data.
3. The gateway authenticates the ADR using data previously obtained from the ACCC's Register.
4. The gateway identifies which data holder(s) hold the consumer's data and provides transaction details to them.
5. The process of authentication and authorisation occurs in accordance with any requirements in the CDR energy rules. The gateway's role in this process is to be determined.
6. The consumer's data is shared with the ADR via the gateway.

In Europe and elsewhere, commercial services are testing different models for trustworthy access to and use of data. These models include the collaboration platform apheris and the PIMS-like service polypoly. With apheris,[32] for example, pharmaceutical data from different participants is made available in encrypted form to carry out decentralized analyses. The function of apheris is to provide a technical platform and application-specific encryption. At polypoly,[33] such an infrastructure is still under construction. It should enable consumers to comprehensively store and manage data on their end devices. Algorithms are planned to learn in a decentralized manner, that is, via federated learning.

32 https://www.apheris.com
33 https://polypoly.org/en-gb/

Risk factor: voluntary or mandatory use of a data trust

Another distinguishing feature of data trust models is whether their use is voluntary or mandatory. As a starting point, it is generally assumed that participants are free to decide whether they want to use a data trust, unless there are special reasons that justify an obligation. In the case of voluntary use, the data trust can be determined via a data trust contract, which is the legal basis of the data exchange.[34] Depending on the sector and application, it may be necessary to set certain limits for the contractual arrangements.

An obligation to use a data trust can be justified by the fact that the objective cannot be achieved through voluntary measures. The objective must warrant regulatory intervention. This need can be driven by various factors, including the following:

- pronounced public interest in the objective pursued by the data trust, for example, due to a close relation with public services (such as health, education, or mobility),
- high concentration in one of the markets in which the data trust is active or a clear imbalance between the parties, so that negotiating power lies predominantly with one party.

The obligation to use a data trust can be imposed in different ways: All parties can be required to put certain data into a data trust or to receive data from a data trust. However, this usually makes sense only for the side(s) that would otherwise probably avoid participating in it. Depending on the constellation, this can be the data-providing side (e.g., car manufacturers in the automotive context) or the data-using side (e.g., digital platforms).

In the case of a mandatory data trust, a higher risk arises because the data trust cannot be circumvented, and the relationship between the participants is strongly interfered with. This means that a problematic design can cause greater damage than a voluntary model. Thus, a mandatory model requires other features of the data trust be chosen with care, such as which prerequisites and conditions of data access and IT security standards the legislator wants to set or leave to be decided by the market. For example, if the data trust is not perceived as trustworthy or if excessive security standards are prescribed, fewer data may be exchanged than would be achieved without a data trust. Too low standards, in turn, can bring abuse by a strong negotiating side and security risks.

An obligation to use a data trust entails further questions, such as whether legal requirements for the conditions for granting access are determined and whether

34 Specht-Riemenschneider et al. (2021), op. cit.

granting access is remunerated.[35] Examining these questions in detail is beyond the scope of this paper.

Restricting only where necessary: The business model

Another design aspect often highlighted is the business model. However, this is not generally a significant risk factor and should not be hastily restricted by regulation. Demands for a "neutral" business model, as articulated in many of the regulatory proposals discussed in Section 3.1., are often unspecific. If neutrality is understood as excluding a profit motive and vertical integration, there is no room for approaches that contribute more strongly to data exploitation and/or can be developed from the data of existing business units. Instead, it is more appropriate to determine which form of neutrality is necessary for a specific application.

Monetization
Data trusts that are not monetized are widely preferred, because this condition would exclude conflicts of interest. This is exemplified by the concept of "data altruistic" organizations in the DGA,[36] which, unlike other data services, should not be subject to general supervision for data services. The election manifesto of the SPD suggests state data trusts and vzbv are also in favor of non-profit foundations and state funding (see Section 3.1.).

However, intermediating, administering, and if necessary, processing data involve effort, which, in turn, is associated with costs. These costs can be covered in various ways. There is the possibility of state funding or subsidization, which means that the costs are passed on to taxpayers. However, private organizations can offer services for a price and make a profit (or loss) on the sales, or they can explicitly be set up as not-for-profit organizations (e.g., through the organizational form of a non-profit limited liability company or a non-profit association).

It is questionable whether excluding a profit motive is necessary or sufficient to ensure the trustworthiness of the data trust. The implicit concern seems to be that the data trust could use data not for the intended purposes, but for the trust's own interests. However, it is unclear what exactly is meant by this concern or to what extent this concern is caused by a profit motive.

35 The proposal for the Digital Markets Act (DMA) includes FRAND (fair, reasonable and non-discriminatory) remuneration for, among others, click data from search engines; see European Commission (2020e), "Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)", Article 6j.
36 European Commission (2020b), "Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)", para. 36.

Figure 3 shows that there is a spectrum of functions and activities that a data trust can perform with data, as well as a spectrum of monetization approaches. The further to the left these functions are, the more likely they are commonly perceived as non-critical. However, activities and business models located on the left tend to place greater restrictions on the extent to which value can be generated from data. Therefore, there is a risk that models will be advocated that are limited to storing data and contribute only a little to gaining new insights through using the data.

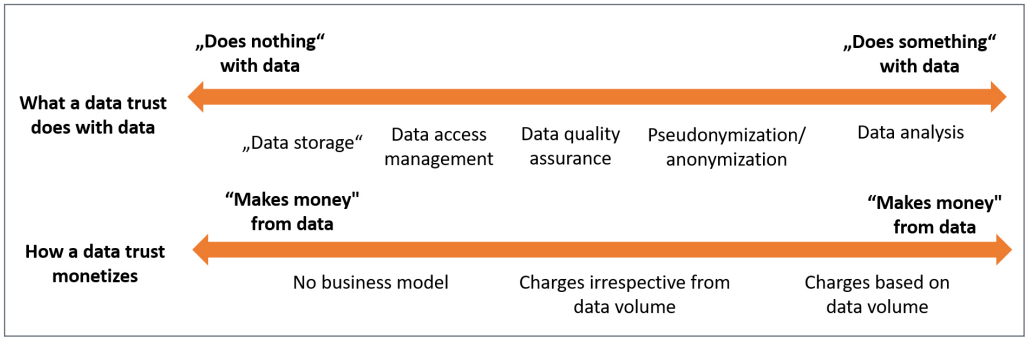

Figure 3: Spectrum of activities and monetization of data trust models

Source: Stiftung Neue Verantwortung

In the context of monetization, a payment dependent on the volume of data is seen as particularly problematic, as it tends to create an incentive to “sell” more data (access) to more data users.[37] At the same time, however, under-utilization, which arises if the data trust is too passive and only incompletely achieves its goal, is also a risk. Under-utilization can occur if access to or exchange of larger amounts of data is desirable, for example, to lower the barriers for new providers of training algorithms. In addition, excluding monetization in principle means that costs may be passed on to the collective to a potentially unnecessary extent (if state funding is used).

Vertical integration

A neutrality requirement in relation to vertical integration is also often neither clear nor reasonable. The Data Governance Act requires data services be separated from other business activities (see Section 3.1.). However, vertical integration is not always problematic, as it does not always lead to discrimination of external services or self-preferencing, and even when it does, self-preferencing is not always problematic. As the Expert Group for the Observatory on the Online Platform Economy noted, unequal treatment of platforms is problematic when providers are powerful, and/or users use only one service, and switching costs are high.[38] In other constellations, a certain degree of vertical integration may be necessary to make certain activities economically viable or scalable.

37 See, for example, vzbv (2020), op. cit.
38 See Graef, Jeon, Rieder, van Hoboken, Husovec (2021), “Work Stream on Differentiated Treatment”, Final report.

Moreover, for a data trust, affiliation with other activities is not always problematic. As stated in Section 3.1., data services can be vertically integrated when an organization decides to make its data available to third parties, possibly combined with data from others. A ban on vertical integration or a requirement for vertical unbundling can prevent such forms of data trust models from emerging. This restriction will certainly prevent possible abuse in cases where a problematic degree of self-preference could arise. However, overall, a ban reduces the scope for possible development paths and business models of data trusts.

Specific rules instead of general neutrality

Instead of a general demand for neutrality, to counteract the risks of certain data trust applications, tailored rules are useful. For example, transparency about revenue sources or separate consent for monetization of data may be useful. In Section 4, we examine these application-specific rules in detail.

In addition, if the business model is restricted in a targeted manner, the data trust's organizational form can still remain open. As with the business models, a spectrum of options can be assumed here, which may have to be restricted according to the specific application. The options for organizational forms range from non-profit organizations to cooperatives to other legal entities and partnerships.

4. Use cases and application-specific regulation

If data trust regulation is to account for risk, it is important to understand application-specific risks and develop regulatory responses. In the following, we look at four areas where increased data sharing is often considered desirable. Data trust models in various forms can be put to use. By looking at the specific challenges and risks, effective measures for regulatory or other policy intervention can be formulated.

The four possible use cases for data trusts are medical data, PIMS, agricultural data, and data for product passports. They represent a spectrum that differs in terms of the relevance of personal data, the extent to which data sharing and use take place, and whether, according to the risk distinction presented in Section 3.1., data storage is central or decentralized, and is shared mandatorily or voluntarily.

For each use case, we examine the status quo, how and to what extent data sharing is taking place. Then we assess the benefits and risks associated with increased data sharing. In the final step, we determine the need for regulation or other policy intervention to balance the benefits and risks.

4.1. Medical data

Status quo

Medical data holds enormous potential for medical research, for example, for the development of new forms of diagnosis and therapy. This can be seen, among other things, in the progress of AI-supported analysis of image data from radiology, for example, by the German companies Smart Reporting[39] and Mediaire.[40] However, existing data sets have been little used. A major reason is the uncertain legal interpretation regarding which forms of data exchange are permitted, and (if strictly interpreted), the prevention of socially desirable data exchange. Specifically, data protection concerns and uncertainties are prominent. At the very least, existing data sets are prohibited from being used for purposes not explicitly listed in the consent. This prevents these data sets from being used for new research purposes that were not foreseeable when the data was collected.

39 Smart Reporting was founded in Munich in 2014 and offers AI-supported image analysis for radiology data. The cloud-based software tool is used by "more than 10,000 doctors in over 90 countries." More information at: https://www.smart-reporting.com/en/company/about

40 Founded in Berlin in 2018, Mediaire builds on AI technology for image data analysis of the brain and spinal cord with the aim of improving diagnosis and treatment quality, as well as enabling more effective workflows in radiology. More information at: https://mediaire.de/

At the same time, there are many efforts to make health data more systematically usable. The medical informatics initiative (Medizininformatik-Initiative) aims to make data from patient care and existing research more accessible. For this purpose, data from clinics should be standardized to enable productive exchange across institutions, and the consent process should, through the use of a standardized form,[41] give patients meaningful options without unnecessarily restricting the scope for research. The introduction of electronic patient records (ePA) is intended to enable data flows among health insurance companies, physicians, and researchers. Since January 2021, patients have been able to request an ePa from their health insurer to fill in with their health data. This data will be released for research purposes beginning in June 2022. The Research Data Centre for Social Data will be further expanded to centrally process the data.

Currently, data from different medical domains has not been cumulatively evaluated. The Cancer Registry and the Transplant Registry represent the first approaches to making data centrally accessible to support data-driven research. The focus for the Cancer Registry is cancer research. Data can be requested via the Centre for Cancer Registry Data (ZfKD) in the form of a scientific use file. This is regulated in the Federal Cancer Registry Data Act (BKRD), which requires that "a justified interest, in particular a scientific interest, is credibly demonstrated."[42] Data in the Transplant Registry can be made available to third parties for research purposes on request since the first quarter of 2021.[43]

Benefits and risks

Increased sharing and use of medical data for research can bring several benefits. Society can gain knowledge about which diseases and factors are interrelated in which ways, and which treatment options work particularly well (or not) for which groups. This knowledge, in turn, is the basis for improved and more personalized treatment for patients that considers individual risk factors. In the context of the coronavirus pandemic, there is evidence that many people are in favor of sharing their data if it will benefit them and/or others.[44]

41 Medical Informatics Initiative (2020), "Consent Working Group Sample Text Patient Consent", available at: "https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf

42 BKRD para. 5, para. 3.

43 https://transplantations-register.de/forschung

44 Dohmen, Schmelz (2021), "Data Protection in the (Corona) Crisis: Focus on Self-Determination and Trust – Policy Paper", available at: https://www.progressives-zentrum.org/wp-content/uploads/2021/05/Datenschutz-in-der-Corona-Krise_Policy-Paper-05_Dohmen-Schmelz.pdf

There are numerous examples of applications, including better detection of rare diseases by pooling data sets to identify patterns that are not apparent when looking at individual cases. The search for patterns is also relevant when studying long-term outcomes of Covid-19; significant resources are being spent on research, including data acquisition.[45] In the case of widespread health problems, such as those that affect the spine, data can help make individual treatment more accurate and safer using imaging data and predict treatment outcomes across patients, information which can be used to select the appropriate treatment.

The risks of increased data sharing are that individual patients and/or specific groups of patients (with common characteristics such as preexisting conditions) can be identified in data sets. This identification negatively affects privacy, which is inherently problematic and can lead to self-censoring behavior, such as not seeking medically necessary information or even treatment.[46] Furthermore, identification can also lead to discrimination: Private health or occupational disability insurances may accept only people with higher risk in worse conditions or not at all. Advertising can also be tailored to certain health characteristics without this being in the interest of the recipient.[47]

If data is used and interpreted inappropriately, large amounts of data can lead researchers to misdiagnose or recommend incorrect treatments. This is particularly the case when correlation of disease patterns is confused with a causal relationship, or when the limitations of data (e.g., non-representative samples) are not sufficiently considered.

There are also concerns that more data sharing will mainly benefit those under scrutiny for potentially problematic data practices. Google and Amazon, for example, are also active in medical business areas.[48] Depending on how more data sharing is designed, it could increase concentration tendencies in such markets.

45 National Institutes of Health (2021), "NIH launches new initiative to study 'Long COVID'", 23 February, https://www.nih.gov/about-nih/who-we-are/nih-director/statements/nih-launches-new-initiative-study-long-covid

46 Marthews, Tucker (2017), "Government Surveillance and Internet Search Behaviour", available at https://ssrn.com/abstract=2412564

47 Lecher (2021), "How Big Pharma Finds Sick Users on Facebook", available at: https://themarkup.org/citizen-browser/2021/05/06/how-big-pharma-finds-sick-users-on-facebook

48 Hurtz (2019), "50 Million Patient Records End Up on Google's Servers", available at: https://www.sueddeutsche.de/digital/google-project-nightingale-gesundheitsdaten-ascension-1.4681463; Cellan-Jones (2018), "Amazon Joins Up with US Firms to Enter Healthcare Sector", available at: https://www.bbc.com/news/business-42877287; Vengattil, Humer (2020), "Alphabet's Verily Targets Employer Health Insurance with Swiss Re Partnership", available at: https://www.reuters.com/article/us-alphabet-verily-idUKKBN25L1Q9

Policy and regulation

The problem of legal uncertainty concerning the exchange of medical data can be solved by creating a clear legal framework for data trusts. The framework should be designed to enable medical research while the risks remain manageable. We propose creating **a legal basis for data processing by scientific and commercial organizations for medical research with data provided by a data trust.**

Data trusts are suitable for encouraging greater data sharing while systematically reducing risks. Ideally, data trusts can give access to currently non-centrally stored data in a way that researchers do not receive the data but train algorithms using the data. However, the data may be centralized compared to the status quo, depending on the data's origin. To make using the data trustworthy, the following elements are appropriate:

- **certification of IT security** by a state-supervised body: Certification is important to protect the data (or data management) from unauthorized access. There are established processes, for example, at the Federal Office for Information Security. In principle, certification of other aspects of data trusts is also possible.[49]
- research project-specific **design of data access in the form of federated learning, aggregation, or pseudonymization:** It is important to limit data access to the extent necessary to realize the desired or hoped-for gain in knowledge. This means that an algorithm can become significantly more precise if it is sent (with the help of federated learning) to large additional data sets without sharing sensitive data. Other forms of research require aggregated data, for example, to test hypotheses about the risk factors of common diseases. However, exploratory research into possible drivers of, for example, rare diseases, is difficult without access to (pseudonymized) individual data.
- a **limitation of data trust status and data access** to (scientific or commercial) institutions that conduct medical research and are not active in one of the areas vulnerable to discrimination (insurance and advertising)[50]: To exclude certain risks with certainty, such as discrimination, this limitation is important. It cannot be ruled out in principle that companies that are also active in the insurance or advertising sector could still pursue socially desirable research purposes. However, it is likely that by excluding such institutions from accessing the data, the gain in patient trust outweighs the potential benefit of sharing data with such organizations.

49 Martin, Pasquarelli (2019), "Exploring Data Trust Certifications", Oxford Insights, available at: https://theodi.org/wp-content/uploads/2019/04/Report_-Exploring-Data-Trust-Certification.pdf

50 See also Hentschel (2021), "DLD Conference: Interview with Stefan Vilsmeier – Data in Medicine: "Diseases can be detected much earlier", available at: https://www.focus.de/digital/dldaily/dld-konferenz-interview-mit-stefan-vilsmeier-daten-in-der-medizin-krankheiten-lassen-sich-viel-frueher-erkennen_id_13012769.html?__blob=publicationFile&v=1h

Medical data (routine data and research data) is processed mainly based on consent solutions. To process routine and research data for purposes beyond those specified in the consent, legal authorization is needed. This legal authorization can permit personal data be processed for scientific research via a data trust. Thus, the data trust replaces alternative broad consent solutions. To protect the legitimate interests of patients, they still need to have the right to opt out. Other processes to ensure patient protection, such as review by an ethics committee, should remain in place.

Although, in principle, using data trusts remains voluntary on the part of the patient, it may make sense to obligate at least some data providers to collaborate. This applies to data collected in the context of publicly funded research and could be extended to other groups such as hospitals. It is also conceivable to create incentives for data-collecting organizations (clinics, medical companies, and others) to participate by establishing reciprocity as a principle. Those who want access to others' data must also provide data themselves (without limiting the patient's right to opt out).

Who can become a data trust is explicitly left open. In view of the great difficulties digitizing public institutions and the research data center,[51] it does not seem very expedient to commission a state agency to fulfill the data trust function. The expertise of technological-medical companies such as Brainlab,[52] a "Google Maps for the operating room," appears indispensable to enable effective data intermediation. Public–private partnerships are also conceivable. Although much speaks in favor of establishing a single data trust organization in the health sector, timely implementation is much more realistic if there is agreement on minimum standards for interoperability between multiple data trusts.

The scope for design of the business model should not be narrowed prematurely, either. Due to the proximity to public services, a justification for (partial) public funding is obvious. At the same time, there is also private-sector interest in greater access to data, which does not necessarily run counter to public interest. This has been shown, among other things, in the development of Covid-19 vaccines. Therefore, companies, too, can at least contribute to funding. It is also conceivable that there could be guidelines for publishing findings obtained with data made available via the data trust. The same applies to requirements for public institutions to provide data. These requirements, however, also concern data access beyond data trusts and should be designed coherently.

51 Federal Institute for Drugs and Medical Devices, "The Research Data Centre", available at: https://www.dimdi.de/dynamic/de/weitere-fachdienste/forschungsdatenzentrum/

52 https://www.brainlab.com

Implementation

To strive for a timely implementation and to keep the hurdles for legal regulation manageable, leeway can first be created for individual areas of research. It may make sense to prioritize areas where medical research is particularly urgent, and data is available. In the United Kingdom, focusing initially on individual areas has led to success. Health Data Research Hubs were established in October 2019 to focus on clearly defined areas: mental health, clinical trial feasibility, cancer care, inflammatory bowel disease, consent-based diagnosis, eye disease, lung and cardiovascular disease, and clinical care.[53] After one and a half years, the initiative has implemented 300 projects, conducted 20,000 interactions with patients and the public, and made 157 data sets available.[54]

In the German system, the Cancer Registry and the Transplant Data Act can serve as reference points. Although they have made data available only within their respective domains, the registry and the legislation include design elements that can be expanded. According to Section 15g of the Transplant Act, access to the Transplantation Register can be granted even without the consent of the person concerned, if obtaining such consent is possible only with disproportionate effort, the public interest in the research outweighs the person's interest, and the research purpose can be achieved only in this way. At the same time, the use of a trust authority (Vertrauensstelle) ensures a minimum level of data protection by pseudonymizing the data by default. In the case of the Cancer Registry, other data is included, at least in part, and highly aggregated results can be viewed without additional hurdles in a database accessible via the website.

It is important that prioritized areas are connected for the development of data trust models, similar to how the Health Data Research Hubs in the UK are centrally coordinated. A minimum level of standardization and interoperability, to be incorporated as early as possible in the design of models, is important so that successful approaches can be scaled up quickly.

53 Health Data Research UK, “Our Hubs”, available at: https://www.hdruk.ac.uk/helping-with-health-data/our-hubs-across-the-uk/

54 Health Data Research UK (2021), “Improving UK Health Data: Impact from Health Data Research Hubs”, available at: https://www.hdruk.ac.uk/wp-content/uploads/2021/04/Improving-UK-Health-Data-Impacts-from-Health-Data-Research-Hubs_compressed.pdf

4.2. PIMS

Status quo

PIMS are not yet a clearly defined group of services. The European Data Protection Supervisor characterizes PIMS as "systems designed to give individuals more control over their personal data."[55] They are often described as data portals through which consumers bring together data from different sources and if appropriate, open up the data to new uses, such as the services/companies digi.me, bitsabout.me, itsmydata, or (in the development phase) polypoly. [56] Also included are consent management systems that allow consumers to set their preferences regarding the collection and use of data about them. These systems are still under development but are being considered for regulatory purposes under the TTDSG and the DGA (see Section 3.1.). Table 2 summarizes the key functionalities and business models of selected active PIMS.

Table 2 Selected active PIMS

Name	Functionalities	(De)Central	Business model	Focus area(s)
Digi.me	Users collect personal data from various platforms and services in the app/website, obtain an overview and can permit possible uses by third parties.	Decentralized storage in the user's cloud	Transaction fee (7.5%)	App is the basis of a data ecosystem of apps developed by third parties, for example, health or travel apps
Bitsabout.me		Central storage on EU servers	Transaction fee	Monetization of personal data by users
Itsmydata		Central storage on German servers	Sale of credit certificate to users; planned: transaction fee	Affordable credit certificate based on data from Schufa, Boniversum, etc.
polypoly		Decentralized storage on the user's device	Planned: software licenses, transaction fee	Cooperative management of technology

Sources: Websites of the service providers

55 Further, the EDPS writes: "Through PIMS, people have the possibility to manage their personal data in secure, local or online storage systems and to share it when and with whom they wish. Online service providers and advertisers will have to interact with PIMS if they intend to process individuals' data. This may lead to a people-centred approach to personal information and also to new business models.", available at: https://edps.europa.eu/data-protection/our-work/subjects/systeme-de-gestion-des-informations-personnelles_de

56 https://www.itsmydata.de; https://www.digi.me; https://www.polypoly.eu; https://www.bitsabout.me

However, use of PIMS has been limited, which can be attributed to their limited functionalities. One reason is the individualistic reading of data rights in the GDPR, which prohibits the delegation of consent or the exercise of rights such as the right to portability. Thus, it is still up to individuals to enforce any granting (or withholding) of consent in a supposedly informed manner.[57]

A form of delegation of rights to PIMS is allowed under the California Consumer Privacy Act (CCPA). This allows consumers to appoint "authorized agents" who can prohibit companies from selling personal data or request it be deleted. Consumer Reports, a U.S. consumer advocacy organization, has piloted[58] such a service and found that there is a clear demand for making data enforcement more effective and easier.[59] A range of organizations offer to act as authorized agents. In principle, the CCPA does not restrict who can take on this role and on what terms. This means that it is up to consumers to choose suitable and trustworthy organizations for their purposes. This approach seems to work, as no cases of abuse are publicly known.

Another reason for the low market penetration of PIMS is that they are voluntary for all parties involved and thus, easy to circumvent. Consumers can "direct" data about themselves to PIMS, but consumers cannot obligate companies to handle the consent process via the PIMS, for example. This means that PIMS have been an additional service for consumers to use alongside manually controlling data flows, instead of being able to at least partially replace manual control via the PIMS.

Benefits and risks

Services that enforce consumers' interests related to data are widely promoted, including by the organization MyData. The potential lies in a data ecosystem in which data flows are more strongly oriented toward consumers' interests. This means that data flows can be limited more effectively, and a desired, uniform level of data protection can be established.[60] However, data flows can be enabled (easily) where they benefit consumers.[61]

57 On the problems of individual consent, see, among others, Blankertz (2020), "Designing Data Trusts".

58 Consumer Reports (2021), "Consumer Reports Study Finds Authorised Agents Can Empower People to Exercise Their Digital Privacy Rights in California", available at: https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-authorized-agents-can-empower-people-to-exercise-their-digital-privacy-rights-in-california/

59 Extensive difficulties in communicating with service providers to get them to respond to requests were also reported. It seems plausible that interested individuals would not have made any further effort in the face of such difficulties, unlike Consumer Reports.

60 _Stiftung Datenschutz (2017), "New Directions in Consent in Data Protection – Technical, Legal and Economic Challenges", available at: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_PolicyPaper_Neue_Wege_zur_Einwilligung_DE_EN_final.pdf

61 Blankertz (2020), op. cit.

At the same time, there are major concerns about whether or which organizations may be considered PIMS or data trusts in the interest of consumers. For PIMS that enable consent management, the TTDSG suggests a corporate foundation as an organizational form and is skeptical about commercial approaches (see Section 3.1.). This skepticism is likely because many services known for problematic data practices conceal those very practices from their users.[62] Thus, in the case of Google, Facebook, and others, it is questionable whether the consumer decision to give consent to these companies to collect extensive personal data is socially desirable. Accordingly, there is a strong political intention to avoid similar dynamics in the creation of new services. However, the example of the authorized agent in the CCPA suggests that a less restrictive approach can also be fruitful.

Excluding possible abuse of power by PIMS as far as possible in advance is sensible. However, no PIMS has established itself in the market, which suggests that developing a service in existing conditions that is attractive to many consumers is challenging. Further restriction through regulation would only reduce the chances of the possible success of PIMS. Instead, regulation that also enables PIMS could help stimulate a critical mass of PIMS services and users.

Policy and regulation

PIMS receive a lot of political attention, most recently with the passing of the TTDSG. However, specific proposals that solve the known hurdles, especially lack of delegation and ease of circumvention, are scarce. We propose **making model terms and conditions for PIMS the basis for certification and mandating companies to cooperate with certified PIMS.**

Certifying terms and conditions can ensure a high, trustworthy minimum standard for PIMS. Certification, carried out by a government agency (e.g., the BfDI or the Bundesdruckerei), comprehensively binds the PIMS to users' interests. Appropriate elements include the following:

1. **Minimum standards for IT security** (similar to those for health data).
2. **Restrictions on monetizing** personal data by the data trust, so that monetization may take place only with explicit consent. If personal data is passed on in return for payment, there should be explicit user consent. To minimize the potential for misuse of non-personal data, the requirement can include data in aggregated or anonymized form, even if disclosing it may be permissible under data protection

62 Forbrukerrådet (2018), "Deceived by Design", available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

law. On the flip side, the consent required for non-monetary data access can be broadened accordingly (e.g., for more general purposes).

3. **Restrictions on data access to affiliated services**: Data access to affiliated services should take place under the same conditions as for external services. This ensures that explicit consent is obtained internally for data that is monetized externally.
4. **Transparency requirements** in relation to monetary and non-monetary data transfers: One option would be to require an easily accessible, constantly updated overview of which organizations are granted access to data with and without payment, with more details on access to data in the case of monetary exchange.

If these standards are met, the risk of data practices that are detrimental to users is significantly reduced. Meeting such standards, in turn, is a prerequisite for granting PIMS stronger powers, such as those provided to authorized agents under the CCPA. The benefits of a PIMS are greater for users if they can delegate the enforcement of their data rights to a greater extent. One way to implement this is to allow PIMS to obtain "broad" consent from users and specifically enforce it against additional parties without requiring the user to be active in every interaction.

To make it more difficult to circumvent data trusts, especially if the data trusts promote the enforcement of data rights, an obligation to cooperate should be imposed on at least certain data-processing services. It can make sense to restrict such an obligation at least in the beginning to avoid high administrative burdens for companies. Starting points could be browser providers and/or target groups of competition regulation, such as addressees of the Digital Markets Act or Article 19a of the Act against Restraints of Competition.[63]

At the same time, the business models of active PIMS providers indicate that overly general requirements for neutrality may make existing approaches inadmissible. All providers listed in Table 2 charge or plan to charge transaction fees, which can be interpreted as an interest in data exchange. In principle, percentage-based transaction fees create an interest in a larger volume of data exchanged via the PIMS. However, in concrete terms, there have been no criticisms of the practices of these PIMS, and some are considered worthy of being further promoted.[64]

63 These two regulations or drafts refer to particularly important services across markets defined according to various criteria, which are subject to higher requirements. See draft bill on the 10th GWB amendment of the Federal Ministry for Economic Affairs and Energy (2021), "Tenth Act Amending the Act against Restraints of Competition for a Focused, Proactive and Digital Competition Law 4.0 (GWB Digitisation Act)" and European Commission (2020e), op. cit.

64 For example, the European Union promotes projects on the use and monetization of personal data with, among others, the DataVaults project, https://www.datavaults.eu/

4.3. Product passports

Status quo

The traceability of products and product characteristics along the value chain is an increasingly important success factor for the economy. Many consumers care about, for example, the production conditions of companies; policymakers promote and demand more sustainable economic activity. One example is the planned creation of a data space for a circular economy, which will feature so-called product passports.[65] Priority is given to sectors with high resource consumption and great potential for increased recycling, such as electronic devices, batteries and cars, packaging, textiles, buildings, and food and water.[66] The variety of priority sectors shows that very different product components and properties can be captured via a data trust.

Various providers offer solutions to make products traceable across supply chains. To enable cross-product or cross-manufacturer solutions, a certain degree of standardization is important. One platform for setting such standards is GS1, an association of numerous international companies that provides standardized barcodes,[67] mainly in the food, health, and transportation sectors.

Benefits and risks

Currently, the demand for product data is driven by end consumers or investors who want to ensure compliance with certain standards. New markets that allocate existing resources more efficiently based on product data and enable the monetization of currently unused resources have played a subordinate role. The intermediation between those who have recyclable resources and those who can use them is complex, especially in the case of cross-sectoral cooperation. It requires platforms such as Excess Materials Exchange, [68] which have established recycling projects in many of the areas prioritized by the EU. In the future, data along the value chain needs to be exchanged and facilitate product development in which subsequent recycling options are considered in early stages.

Increasing transparency through product passports is potentially valuable for many stakeholders. It is a prerequisite (though not a sufficient condition) to ensure compliance with standards. Risks and disadvantages arise for those who benefit from

65 European Commission (2020a), “Appendix to the Communication 'A European Strategy for Data'”, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

66 _European Commission (2020c), “Circular economy action plan”, available at: https://ec.europa.eu/environment/strategy/circular-economy-action-plan_en

67 https://www.gs1.org/about

68 https://excessmaterialsexchange.com/en_us/

non-transparency, or if inefficient standards are set. In addition, imbalances within the value chain could be reinforced if transparency is guaranteed only unilaterally or the efficiency gains are appropriated by only the stronger negotiating partner (e.g., by negotiating stricter supply conditions). Imbalances in standardization could also come into play if large suppliers impose requirements that disadvantage smaller ones. However, the main concern is to create a standard that is as inclusive as possible, because high fragmentation could jeopardize the success of product passports. The risks seem limited, and the challenge is to enable data exchange.

There are two major hurdles to greater traceability across value chains. First, the administrative and financial effort of digitizing supply and production processes is often considerable. Second, it is often understood as a primarily administrative task that tends to be given low priority by management or especially for small companies, exceeds available resources. This applies even when the benefits go beyond only more transparency for buyers and end-customers such that the data can generate positive value, that is, however, not critical to the business. Both hurdles are likely to be temporary, as digitization and data collection within companies seem inevitable, and poor data availability is one of the main reasons for the high management effort.

Policy and regulation

It is not evident that there is a need for restrictive regulation for data trusts that want to offer product passports. For example, to what extent centralized or decentralized models should be used remains open, and it may vary depending on the product and function. Cases of abuse or other negative consequences by product data intermediaries are not known. From a competition policy perspective, a need to balance policy objectives may arise if a company uses its market power to enforce higher sustainability standards in supply chains.

Instead, the question is to what extent the development of transparency in the form of product passports can be promoted, because companies have been reluctant to make their products more traceable. One enabling element is the inspection of data cooperation under antitrust law, which since the 10th German Competition Act amendment is to take place within a maximum of half a year by the Federal Cartel Office.[69] In addition, the state can promote the development of data exchange in certain areas, as is done at the EU level through pilot projects in the context of the Circular Economy Data Space. Another instrument is the strategic creation of demand by the state via procurement standards, for example, of construction projects, in which product passports can become a necessary prerequisite. This would make

69 Act against Restraints of Competition, Section 32c.4.

the use of such a data trust, in certain circumstances, not purely voluntary but partly mandatory. The same applies to possible sustainability reporting requirements imposed on companies by the state and/or financial markets. These requirements can lead to sustainability gaining relevance in supply chains and internal processes.

4.4. Agricultural data

Status quo

Data from and for agriculture comes from a variety of sources, from sensors in the soil and machines to weather and climate data to economic developments in the global market.[70] The focus is often on machine data, whose compatibility, access, and further use are discussed worldwide, from Australia[71] to the USA[72] to Europe.[73] The level of digitization of machinery is quite high, and much data is collected by default without farmers having to make any further efforts.

Benefits and risks

Some farms use machine and other data to tailor management more closely to the condition of sub-field areas, for example, with fertilizers or water (also known as precision farming). There is clear potential not only to increase yields but also to use resources more effectively. For example, data for individual machines can be calibrated to work different areas of a field differently.

Currently, data is collected and used in individual farms without any exchange across farms. This means that each company learns only from its own data, and no comprehensive analyses are carried out.

To enable cross-company analyses, there are two prerequisites: First, to be meaningfully analyzed, data must be available in an exchangeable format. The process of standardization is underway, and organizations such as agrirouter, for example, are working on solutions that enable cross-machine manufacturer data processing.

70 Wolfert, Ge, Verdouw, Bogaardt (2017), "Big Data in Smart Farming – A Review", Agricultural Systems, Volume 153, pages 69-80, available at: https://www.sciencedirect.com/science/article/pii/S0308521X16303754

71 Wiseman, Sanderson (2017), "The legal dimensions of digital agriculture in Australia: An examination of the current and future state of data rules dealing with ownership, access, privacy and trust", available at: https://www.crdc.com.au/sites/default/files/CRD18001-001%20CRDC%20P2D%20Report%20low%20res.pdf

72 American Farm Bureau Federation (2016), "Privacy and Security Principles for Farm Data", available at: https://www.fb.org/issues/innovation/data-privacy/privacy-and-security-principles-for-farm-data

73 an der Burg, Wiseman, Krkeljas (2020), "Trust in Farm Data Sharing: Reflections on the EU Code of Conduct for Agricultural Data Sharing", Ethics and Information Technology, available at: https://link.springer.com/article/10.1007/s10676-020-09543-1

Agrirouter acts as a platform between many machine manufacturers, connecting software providers to farmers via standardized interfaces.

Second, there must be a willingness to exchange data. This is a challenge partly due to a lack of digitalization and data use on the farms themselves (even if the data is collected in the machines). Furthermore, the risks are often perceived as more concrete than the potential benefits of better trained agricultural software. These risks include the disclosure of trade secrets, such as yields and agricultural practices. In the German context, the power and information imbalance between machine manufacturers and farmers does not appear to be practically relevant, although this issue is occasionally mentioned in the literature.[74]

Policy and regulation

In reference to the planned EU data spaces, the so-called "Agri-Gaia" is being developed by the German Federal Ministry for Economic Affairs and Energy. Among other things, this platform intends to promote data sharing between stakeholders, although to what extent this will include cross-farm analyses is not known. It can be assumed that the project will develop into a primarily decentralized data trust, the

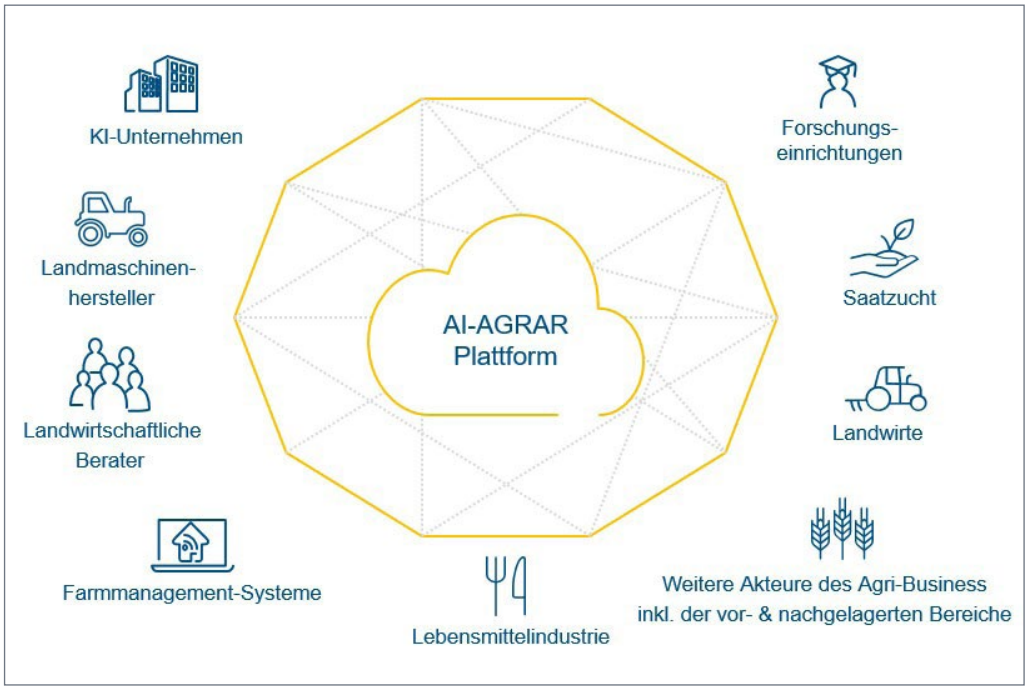

Figure 4: Stakeholders of the AI agriculture platform

Source: Federal Ministry for Economic Affairs and Energy, "Agri-Gaia", available at: https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/GAIA-X-Use-Cases/agri-gaia.htm

74 Zscheischler et al. (2021), "Chapter 4 Agriculture, Digitisation and Digital Data", in DiDaT White Paper, available at: https://www.researchgate.net/publication/349557077_Kapitel_4_Landwirtschaft_Digitalisierung_und_digitale_Daten

use of which will be predominantly voluntary. This goes hand in hand with the low-risk profile of the data exchange, which speaks for low regulatory intensity.

However, incentives for the use of a data trust could be considered. Some farmers would like to see better provision of relevant data by the state, for example, accurate geospatial data including environmental regulatory requirements. As shown in Figure 4, government agencies do not appear as providers of data in Agri-Gaia. However, the added value generated by the state by providing such data through a data trust could certainly lower the barriers for farmers to collect and provide data themselves.

In addition, monetary incentives are conceivable. For example, it is not uncommon to tie the continued payment of some subsidies to certain conditions. Providing anonymized data could be such a condition.

5. Conclusions for the design of data trust regulation

Data trusts can take many different forms to combine data use and data protection, and where appropriate, additional objectives. Current regulatory proposals risk making the scope for companies and other organizations that are or can become active as data trusts too narrow. These projects, especially the DGA, formulate general requirements that often are not necessary for specific use cases.

If policymakers want to contribute to establishing data trusts, they should promote trustworthiness through regulation that considers the risks of specific use cases. Risk factors can be identified across sectors; in particular, centralized or decentralized data storage and the voluntary or mandatory use of data trusts are among the risks. The business model is not a major risk factor. Although the regulatory proposals generally demand neutrality, various data trusts appear trustworthy even without strict neutrality in terms of monetization or vertical integration. At the same time, it is unclear what incentives exist for the development of strictly neutral data trusts.

In addition, recommendations for the design of effective regulation of data trusts emerge from the consideration of the four use cases:

The use cases show a wide range of approaches pursuing different objectives and with specific challenges. Regulation should not establish a supposedly optimal model, especially in the absence of incentives to implement such a model. Instead, regulation should address actual risks and problems.

- For the two use cases without significant use of personal data (agricultural data and product passports), it is questionable to what extent regulation makes sense, as the main challenge is a lack of incentives to establish greater data sharing and/or new models.
- In the two use cases with personal data (medical data and PIMS), there are partly different objectives and risks that require targeted measures.

Regulation should not increase existing legal uncertainty and complexity but reduce it. This is necessary to create an incentive to develop new models.

- Trust-building measures that safeguard against risks warrant the reduction of other hurdles. This is the case, for example, with a health data trust that allows data to be used for medical research even without consent. Similarly, PIMS may be allowed to represent users more comprehensively if other safeguards are in place to prevent misuse.

- Overly restrictive neutrality requirements inevitably lead to data trusts provided by the state, which can be problematic for various reasons depending on the use case. Neutrality in terms of monetization and vertical integration do not reflect the reality of existing PIMS and other data trusts. Provisions to avoid specific conflicts of interest, such as excluding insurance companies and advertisers in the context of a medical data trust, are preferable.

Certification can be a useful instrument to increase transparency regarding defined requirements. Certification can be used where the risk of overly restrictive regulation is too high, but there is a clear need for intervention, for example, due to information asymmetries.

- Certification is an established tool for IT security and can be particularly useful where consumers use the services, as consumers tend to have less expertise and resources to assess a provider. This is especially the case with medical data and PIMS.
- For PIMS, certification of terms and conditions is a way to increase the trustworthiness of services without banning services that do not meet certain criteria. This applies, for example, to full transparency of data monetization and equal treatment of vertically integrated services.

A pragmatic way to promote data trust models is through pilot projects and strategic use of government demand.

- The stipulation of authorized agents in the CCPA shows that the representation of consumers by, for example, PIMS can be a useful instrument for strengthening data rights.
- The UK experience with Health Data Research Hubs shows that it is possible to prioritize certain health data to improve data sharing in specific areas, without creating an all-encompassing database.
- In the area of product passports for the circular economy, government demand can be a strong driver for the spread of product passports for certain products.

In summary, there are many ways to promote the development of data trusts to make data use and data protection more compatible. However, the current regulatory proposals tend to be counterproductive. Regulation should focus on specific risks that are not covered by the existing legal framework and consider lowering some hurdles if additional regulation sufficiently addresses the risks.

Bibliography

ACCC (2019), "Consumer Data Right in Energy – Position Paper: data access model for energy data", available at: https://www.accc.gov.au/system/files/ACCC%20-%20CDR%20-%20energy%20-%20data%20access%20models%20position%20paper%20-%20August%202019.pdf

ACCC (2020), "Energy Rules Framework – Consultation Paper", available at: https://www.accc.gov.au/system/files/CDR%20-%20Energy%20rules%20framework%20consultation%20paper%20-%20July%202020_0.pdf

American Farm Bureau Federation (2016), "Privacy and Security Principles for Farm Data"

an der Burg, Wiseman, Krkeljas (2020), "Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing", Ethics and Information Technology, available at: https://link.springer.com/article/10.1007/s10676-020-09543-1

Blankertz (2020), "Designing Data Trusts – Why We Need to Test Consumer Data Trusts Now"

Blankertz, von Braunmühl, Kuzev, Richter, Richter, Schallbruch (2020), "Datentreuhandmodelle", available at: https://www.ip.mpg.de/de/publikationen/details/datentreuhandmodelle-themenpapier.html

Bundesdruckerei, iRights (2019), "Zukunft Gesundheitsdaten", available at: https://www.bundesdruckerei.de/system/files/dokumente/pdf/Studie_Zukunft-Gesundheitsdaten.pdf.

German Federal Government (2021), "Data strategy of the German government" Jan.

Cellan-Jones (2018), "Amazon joins up with US firms to enter healthcare sector", available at: https://www.bbc.com/news/business-42877287

Consumer Reports (2021), "Consumer Reports study finds authorized agents can empower people to exercise their digital privacy rights in California", available at: https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-authorized-agents-can-empower-people-to-exercise-their-digital-privacy-rights-in-california/

Data Ethics Commission (2019), "Expert Opinion of the Data Ethics Commission"

Deutsche Bundesbank, "Research Data and Service Center (FDSZ)", available at: https://www.bundesbank.de/de/bundesbank/forschung/fdsz/forschungsdaten-und-servicezentrum-fdsz--604430

Dohmen, Schmelz (2021), "Data Protection in the (Corona) Crisis: Focus on Self-Determination and Trust – Policy Paper", available at: https://www.progressives-zentrum.org/wp-content/uploads/2021/05/Datenschutz-in-der-Corona-Krise_Policy-Paper-05_Dohmen-Schmelz.pdf

European Commission (2018), Case M.8744 -DAIMLER / BMW / CAR SHARING JV, November 7.

European Commission (2020a), "Appendix to the Communication 'A European strategy for data", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

European Commission (2020b), "Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)"

European Commission (2020c), "Circular economy action plan", available at: https://ec.europa.eu/environment/strategy/circular-economy-action-plan_en

European Commission (2020d), Case AT.40462 Amazon Marketplace.

European Commission (2020e), "Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)"

European Commission (2021), "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence", available at: https://ec.europa.eu/newsroom/dae/redirection/document/75788

Federal Institute for Drugs and Medical Devices, "The Research Data Center", available at: https://www.dimdi.de/dynamic/de/weitere-fachdienste/forschungsdatenzentrum/

Federal Ministry for Economic Affairs and Energy (2021), "Tenth Act Amending the Act against Restraints of Competition for a Focused, Proactive and Digital Competition Law 4.0 (GWB Digitalization Act)"

Forbrukerrådet (2018), "Deceived by Design," available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

German Bundestag (2021), "Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Energie zu dem Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien", Drucksache 19/29839, available at: https://dip21.bundestag.de/dip21/btd/19/298/1929839.pdf

German Council for Information Infrastructures (2021), "Workshop Report of the Data Trustship WG – Data Trusts: Potentials, Expectations, Implementation."

German Insurance Association (2018), "Datenkranz beim automatisierten Fahren gemäß § 63a StVG – externe Speicherung bei einem Datentreuhänder", position paper, August.

Graef, Jeon, Rieder, van Hoboken, Husovec (2021), "Work Stream on Differentiated Treatment", Final report.

Graf von Bernstorff (2011), "Einführung in das englische Recht", 4th ed.

Health Data Research UK (2021), "Improving UK Health Data: Impact from Health Data Research Hubs", available at: https://www.hdruk.ac.uk/wp-content/uploads/2021/04/Improving-UK-Health-Data-Impacts-from-Health-Data-Research-Hubs_compressed.pdf

Health Data Research UK, "Our Hubs", available at: https://www.hdruk.ac.uk/helping-with-health-data/our-hubs-across-the-uk/

Hentschel (2021), "DLD Conference: Interview with Stefan Vilsmeier – Data in Medicine: Diseases can be detected much earlier", available at: https://www.focus.de/digital/dldaily/dld-konferenz-interview-mit-stefan-vilsmeier-daten-in-der-medizin-krankheiten-lassen-sich-viel-frueher-erkennen_id_13012769.html?__blob=publicationFile&v=1h

Hurtz (2019), "50 Million Patient Records End Up on Google's Servers", available at: https://www.sueddeutsche.de/digital/google-project-nightingale-gesundheitsdaten-ascension-1.4681463

Kerber (2018), "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data," JIPITEC 9 (3).

Kerber (2021), "DGA – some remarks from an economic perspective", available at: https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/pdf-dateien/kerber_dga_einige-bemerkungen_21012021.pdf

Lecher (2021), "How Big Pharma Finds Sick Users on Facebook", available at: https://themarkup.org/citizen-browser/2021/05/06/how-big-pharma-finds-sick-users-on-facebook

Marthews, Tucker (2017), "Government Surveillance and Internet Search Behavior", available at: https://ssrn.com/abstract=2412564

Martin, Pasquarelli (2019), "Exploring Data Trust Certifications", Oxford Insights, available at: https://theodi.org/wp-content/uploads/2019/04/Report_-Exploring-Data-Trust-Certification.pdf

Medical Informatics Initiative (2020), "Consent Working Group Sample Text Patient Consent", available at: " https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf

National Institutes of Health (2021), "NIH Launches New Initiative to Study "Long COVID", February 23, https://www.nih.gov/about-nih/who-we-are/nih-director/statements/nih-launches-new-initiative-study-long-covid

Nitschke (2018), "Microsoft to provide its cloud services from new data centers in Germany starting in 2019 in response to changing customer demands", available at: https://news.microsoft.com/de-de/microsoft-cloud-2019-rechenzentren-deutschland/

Schwartmann, Hanloser, Weiß (2021), "PIMS in the TTDSG – Proposal for regulating consent management services in the Telecommunications Telemedia Data Protection Act", March.

SPD (2021), "Das Zukunftsprogramm der SPD", available at: https://www.spd.de/fileadmin/Dokumente/Beschluesse/Programm/SPD-Zukunftsprogramm.pdf

Specht, Kerber (2017), "Datenrechte – eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA", Abida-Gutachten, available at: https://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf.

Specht-Riemenschneider, Blankertz, Sierek, Schneider, Knapp, Henne (2021), "Datentreuhand: Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle" Supplement in MMR, June.

Stiftung Datenschutz (2017), "New Directions in Consent in Data Protection – Technical, Legal and Economic Challenges", available at: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_PolicyPaper_Neue_Wege_zur_Einwilligung_DE_EN_final.pdf

Vengattil, Humer (2020), "Alphabet's Verily targets employer health insurance with Swiss Re partnership", available at: https://www.reuters.com/article/us-alphabet-verily-idUKKBN25L1Q9

vzbv (2020), "Personal Information Management Systems (PIMS): opportunities, risks and requirements", Feb.

Wendehorst, Schwamberger, Grinzinger (2020), "Datentreuhand -wie hilfreich sind sachenrechtliche Konzepte?", in Pertot (ed.), Rights to Data.

Wiseman, Sanderson (2017), "The legal dimensions of digital agriculture in Australia: An examination of the current and future state of data rules dealing with ownership, access, privacy and trust", available at: https://www.crdc.com.au/sites/default/files/CRD18001-001%20CRDC%20P2D%20Report%20low%20res.pdf

Wolfert, Ge, Verdouw, Bogaardt (2017), "Big Data in Smart Farming – A review", Agricultural Systems, Volume 153, pages 69-80, available at: https://www.sciencedirect.com/science/article/pii/S0308521X16303754

Zscheischler et al. (2021), "Chapter 4 Agriculture, Digitization and Digital Data" in DiDaT White Paper, available at: https://www.researchgate.net/publication/349557077_Kapitel_4_Landwirtschaft_Digitalisierung_und_digitale_Daten

Internet links (last accessed on 01.06.2021)

https://edps.europa.eu/data-protection/our-work/subjects/systeme-de-gestion-des-informations-personnelles_de

https://excessmaterialsexchange.com/en_us/

https://polypoly.org/en-gb/

https://siemens.mindsphere.io

https://transplantations-register.de/forschung

https://www.apheris.com

https://www.bbc.com/news/business-42877287

https://www.bitsabout.me

https://www.brainlab.com

https://www.datavaults.eu/

https://www.digi.me

https://enid.foundation/

https://www.gs1.org/about

https://www.home-connect-plus.com/de/app/

https://www.itsmydata.de

https://mediaire.de/

https://www.polypoly.eu

https://www.smart-reporting.com/en/company/about

https://www.tonysopenchain.com/

Acknowledgements

Many thanks to everyone who has provided input into the paper, including to the many experts at companies, universities and research organizations, regulators, and ministries who shared their insights. Our particular thanks go to Luis Hopf, Brainlab, Wolfgang Kerber, University of Marburg, Walter Pasquarelli, Open Data Institute, Alexander Radbruch, University Hospital Bonn, Stephan Ramesohl, Wuppertal-Institut, Ingrid Schneider, University of Hamburg, as well as to our colleagues, especially Theresa Henne and Julian Jaursch (SNV) and Jakob Knapp, Ruben Schneider (University of Bonn) and Pascal Sierek (Osborne Clarke). The views in this paper do not necessarily reflect those of the experts we spoke with, and all errors are our own.

About the Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent, non-profit think tank working at the intersection of technology and society. The core method of SNV is collaborative policy development, involving experts from government, tech companies, civil society and academia to test and develop analyses with the aim of generating ideas on how governments can positively shape the technological transformation. To guarantee the independence of its work, the organization has adopted a concept of mixed funding sources that include foundations, public funds and corporate donations.

About the Authors

Aline Blankertz leads the project "Data Economy" and assesses economic, technical and social issues in order to develop innovative data policy recommendations. Before joining Stiftung Neue Verantwortung, Aline led economic analyses of the platform economy, among others into competition, data protection and algorithms.

Prof. Dr. Louisa Specht holds the Chair of Civil Law, Information and Data Law at the University of Bonn, heads the Research Center for Legal Issues of New Technologies and Data Law (ForTech), and is deputy chairwoman of the Council of Experts on Consumer Protection at the Federal Ministry of Justice and Consumer Protection.

Contact the Authors:

Aline Blankertz
Project Manager Data Economy
ablankertz@stiftung-nv.de
+49 (0)30 40 36 76 98 1

Louisa Specht
sekretariat.specht@jura.uni-bonn.de
@louisa_specht
+49 (0)228 73 42 40

Imprint

Stiftung Neue Verantwortung e.V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Jan Klöthe