The Data Governance Act – Is "Trust" the Key for Incentivising Data Sharing?

Lucie Antoine

Abstract

In order to contribute to the overall objective of fostering data sharing in the EU, the Data Governance Act introduces two sets of provisions: first, it provides a standardised procedural mechanism for facilitating the re-use of certain data categories held by public sector bodies; second, it establishes a legal framework for the provision of data intermediation services in general and data altruism organisations in particular. Thereby, the Data Governance Act heavily builds upon the idea of increasing trust. During the last years, the principle of trust has already become a central regulatory objective in EU legislation, in particular as regards the online and platform environment. However, which role can trust play in the data economy for incentivising data sharing? And can the Data Governance Act, following this rationale, fulfil its objectives from both a theoretical and practical perspective?

1. The role of trust for data sharing

Does trust play an essential role in incentivising data sharing? Is increasing trust in data intermediaries the key for fostering the development of respective actors in the European market? And can the establishment of trustworthy data intermediaries contribute significantly to the overall objective of creating a European single market for data by enhancing the availability and reusability of data?

Following the underlying rationale of the Data Governance Act (DGA) (Regulation (EU) 2022/868), these three questions would have to be answered in the affirmative. Trust is the general principle shaping the DGA. Indeed, it seems clear that this holds true for the DGA's provisions defining a mandatory legal framework for *data intermediation services* in general and *data altruism organisations* in particular (see Section 3.0.). Data intermediation services, such as platforms allowing businesses to exchange data,

and data altruism organisations, including initiatives pooling health data in order to make it available for scientific research, should provide their services in a manner that users or data *donors* can be sure that *their* data is only used for the intended purposes, and not, for instance, for the business interests of the provider. Introducing legally binding conditions for offering data intermediation or altruism services thus aims – in a first step – to foster the development of reliable, neutral, and therefore trustworthy data intermediaries in line with *European values*. High hopes have been expressed that – in a second step – data intermediaries can then increase trust in data sharing as such, making data flow more easily in practice.

Moreover, the DGA's second important set of provisions on facilitating the re-use of data held by public sector bodies builds upon the principle of trust equally (see Section 3.0). These provisions address constellations in which public sector bodies (e.g., statistical offices) possess data (e.g., statistical data) intended to be re-used by third parties (e.g., for scientific research). By defining standardised and transparent conditions for requesting access and re-use of data held by the public sector, trust in both the re-use mechanism and the acting institution should be strengthened. This is particularly important as the DGA addresses the re-use of data protected on grounds of commercial or statistic confidentiality, by intellectual property (IP) rights of third parties or as personal data. As such, the DGA introduces instruments that account for the data's sensitivity, e.g., by restricting the transfer of certain data to third countries outside the EU.

Even though, on principle, it is convincing that trust has been identified as a pivotal prerequisite for data sharing (European Commission, 2018, p. 1; Richter and Slowinski, 2019, p. 14), the DGA and its underlying rationale raise manifold questions on the general concept of trust (from a sociological and a legal perspective) and its relation to data sharing requiring more nuanced inquiries, particularly from an interdisciplinary perspective. This ranges from highly fundamental aspects on law and trust over the role of trust as a guiding principle for the European platform economy (see Section2) to the specific question of whether the DGA's provisions, which rely heavily on the principle of trust (see Section 3.), can fulfil their objective from both a theoretical and practical perspective (see Sections 3 and 4.).

2. Law and trust

Trust can be defined as the "firm belief in the reliability, truth, or ability of someone or something" (Oxford English Dictionary, 2024). From a sociological perspective, Luhmann (2014, pp. 27, 39) influentially considered trust as the pre-requisite for reducing (social) complexity. This concerns in particular the complexity arising from the *freedom* of others to behave in a way that might run counter to the trusting party's expectations (Luhmann, 2014, p. 38). Trust goes beyond *information* as it is not possible to predict a counterpart's behaviour with sufficient certainty (Luhmann, 2014, p. 38). However, social – and legal – norms can provide objective reference points for anchoring trust (e.g., through sanctions). Such frameworks have the result that certain (on principle, possible) actions are deemed less probable, which can impact decision making (Luhmann, 2014, pp. 29, 40). Accordingly, trust and law are strongly interconnected (Peukert, 2022, p. 231). Put simply, the law (i.e., legal norms) can contribute to minimising *risk* by reducing uncertainty, and is therefore a factor that can increase *trust*. Legally speaking, trust consequently plays an important role as a theoretical justification for normative intervention in form of laws (cf. Peukert, 2022, p. 232). Trust shall be created *through* the law – however, at the same time, this depends on trust *in* the law (Peukert, 2022, p. 231) and its institutions.

As Luhmann (2014, p. 24) already posited, the more complex systems become, the more trust is required. Along these lines, trust has, in recent years, become a central regulatory objective in EU legislation, particularly in terms of the (highly complex) online and platform environment (Peukert, 2022, p. 237; Cole, 2022). The online environment does not only consist of a multitude of actors that, in part, have assumed genuinely *new* roles in society (most importantly, platforms and intermediaries), it also offers a plethora of possible ways for behaving. This increases complexity and, thus, risk, which could lead to low levels of trust. In particular, the Digital Services Act (DSA), introduced as Europe's "basic law for the platform economy", strongly refers to the principle of trust (see, e.g., Cole, 2022, p. 308; Kaesling, 2022). In order to create a "trusted online environment", inter alia hate speech (Liesching, 2022) and disinformation (Peukert, 2023) have been regulated. *Trusted flaggers* should contribute to identifying *illegal content*, both under the DSA (Kaesling, 2022) and, for copyright infringing content, under the Digital Single Markets Directive (DSM Directive; see Lauber-Rönsberg, 2022). Furthermore, comparably early instruments,

such as the E-Commerce Directive (2000/31/EC) or the Platform to Business Regulation (2019/ 1150), already contain strong references to "trust" and "trustworthiness" (for further examples, see Cole, 2022, p. 320). The European regulation of AI is characterised by a comparable approach aimed at creating and promoting "trustworthy AI" (see AI Act[1], Regulation 2024/1689). However, also on a global level, the vision of a "trusted" digital future (OECD, 2022b) and "fostering data flows with trust" (OECD, 2022a) is shared.

3. Trust in the DGA

3.1 The DGA: background, legal nature, and overview

As a legal instrument, the DGA is tailored to increase trust in actors that have been identified as relevant for allowing data to flow in Europe, thus contributing to the overarching objective to establish a European data economy. In order to unleash the full potential of data-driven innovation in the EU, the European Data Strategy (European Commission, 2020a) follows an approach of openness and access to data. The overall aim is to facilitate data sharing between different actors, and thus establish a European single market for data. The majority of legal instruments implemented in recent years have primarily pursued the objective that data can be accessed, ported, and re-used: the Open Data Directive (ODD), regarding the re-use of certain data held by the public sector (G2B); the Data Act (DA), addressing data access in particular in B2B and B2C relations, as well as access to privately held data by the public sector (B2G); the Digital Markets Act (DMA), providing – inter alia – access and portability rights vis-à-vis gatekeepers; the General Data Protection Regulation (GDPR), covering access to and portability of personal data; and the Digital Content Directive (DCD), enabling consumers to port certain non-personal data (as part of further contractual rights and obligations in relation to digital content).

However, both these mandatory instruments and voluntary data sharing (mostly based on contracts) face a common challenge: *how* can the envisaged data flows be made to effectively work in practice? Not only legal uncertainty – particularly regarding personal data – but also organisational

1 For more information on trustworthy AI in the AI Act, see Chapter 3 'Accountable AI: It Takes Two to Tango' by Jorge Constantino.

(infrastructure) and technical (e.g., standardisation, interoperability) barriers constitute relevant practical obstacles for data sharing (see Leistner and Antoine, 2022, p. 34). To this list, the DGA adds the lack of trust – in processes, in actors, in the ability to maintain control over data, and in data sharing in general.

The DGA therefore repeatedly refers to the principle of trust (Kerber, 2021, p. 2).[2] Strengthening trust in the data economy and in the concept of data sharing as an important means for fostering the data economy requires trust in the involved actors, whether the public sector, businesses, or individuals. The DGA identifies transparency and "trustworthy" data governance structures as the main factors by which to increase trust in the relevant players, accompanied by guaranteeing control over data by the individual data subject or data holder.

However, the DGA does not lay down a general horizontal framework for data governance in the strict sense. Rather, it focuses on more specific areas: *first,* the DGA implements a standardised mechanism for facilitating the re-use of data held by public sector bodies that cannot be made available as open data due to its sensitive character (see Section 3.0); *second*, the DGA provides a legal framework for data intermediation services in general and for data altruism organisations in particular, which have been identified as important enablers for facilitating data sharing in practice (see Section 03.3). These provisions exemplify the DGA's underlying rationale that increasing trust is deemed key for fostering data sharing.

The DGA also contains further provisions on the competent national authorities, the international transfer of non-personal data, and the establishment of a European Data Innovation Board (EDIB); however, this chapter will not address these provisions in detail.

The DGA entered into force on 23 June 2022 and has been applicable since 24 September 2023. As the DGA is a Regulation, its provisions are directly applicable in the Member States without having to be transposed into national law.

2 See Recitals 3, 5, 23, 24, 32, 33, 38, 43, 46, 47, and 52 DGA.

3.2 Re-use of public sector information (Chapter II): trust in the process and in the institutions

With the provisions contained in Arts. 3–9, the DGA introduces a standardised procedural mechanism for facilitating the re-use of certain data categories held by public sector bodies. The term *re-use* is broadly understood as referring to use by natural or legal persons for non-commercial and commercial purposes (Art. 2(2) DGA). In a nutshell, the DGA's provisions in Chapter II aim at making data (subject to the rights of third parties) held by the public sector available for re-use while respecting their sensitive nature at the same time (Kerber, 2021, p.1). The principle that data which has been collected by public sector bodies at the expense of public budgets should benefit society has been part of EU policy for a long time (Recital 6 DGA) and is manifested in, for example, the legal instruments on open data. However, where data of a more sensitive nature is at stake, public sector bodies must also respect that particular character as part of their public task.

The DGA does not address the question as to *whether* data held by the public sector body should be made available for re-use, but rather *how* making data available for re-use should work (Lauber-Rönsberg and Becker, 2023, p. 32). Establishing a basic procedural framework for data re-use requests and laying down conditions for re-use intended to protect the data's sensitive character has the objective to increase transparency. Consequently, citizens can trust public sector bodies that they, on the one hand, do not *retain* data that are valuable for research or innovation purposes, while they, on the other hand, comply with their public task by preserving the data's sensitive nature, even when making them available for re-use.

The DGA has been inspired by the re-use mechanisms that certain Member States already have in place (Richter, 2022, p. 4). The European Commission's (EC) Impact Assessment Report (European Commission, 2020b, p. 13), for instance, refers to the French "Centre d'accès sécurisé aux données" (Centre for secure access to data) established inter alia by the French government and the National School for Statistics, allowing the secure processing of statistical micro-data. It also refers to the establishment of the data permit authority "Findata" in Finland, which provides a one-stop shop solution for data re-use requests as well as to research centres established in Germany for facilitating access to medical reimbursement data for researchers by providing a "secure data research infrastructure".

Bearing these envisaged mechanisms in mind can certainly help to better understand the DGA's provisions in detail.

3.2.1 Scope and covered data categories

According to Art. 3(1), the DGA applies to data held by public sector bodies that are protected on grounds of commercial or statistic confidentiality, by IP rights of third parties or as personal data ("protected data", see European Commission, 2024a, p. 2). Thus, the DGA addresses data that does not fall within the scope of the ODD precisely because of its *sensitivity* (cf. Art. 3(1), Recital 10 DGA; Baloup et al, 2021, p. 17; Richter, 2022, pp. 4, 7). For instance, data that has to be made available to a public sector body based on a legal obligation to disclose certain information may also qualify as trade secrets.

Addressees of the provisions are public sector bodies, i.e., a state, regional or local authorities, or other bodies governed by public law (see definitions in Art. 2(17) and Art. 2(18) DGA).[3] The DGA points at data the public sector body supplies as part of its public task (Recital 12, cf. Art. 3(2) (e) DGA). This means that a public sector body is – from a technical and factual perspective – competent for granting access to data for re-use (Specht-Riemenschneider in Specht-Riemenschneider and Hennemann, 2023, Art. 3 para. 62). In fact, it will often primarily depend on whether a public sector body is – in a first step – competent for collecting and storing respective data (Specht-Riemenschneider in Specht-Riemenschneider and Hennemann, 2023, Art. 3 para. 62). Thus, the addressees of the provisions are public sector bodies competent under national law for granting or refusing access requests for re-use (Art. 5(1) DGA). A rather simple example would be a statistical office that makes certain statistical data available for re-use in research or commercial applications.

The DGA itself neither introduces access rights nor obliges Member States to make the data in scope available for re-use (Recital 11 DGA).[4] Rather, it depends on the Member States' national law whether and which publicly held data will be accessible for re-use, under which conditions, and for which purposes.

3 See exception in Art. 3(2) DGA for data held by public undertakings, public service broadcasters, and cultural or educational institutions, such as museums, libraries, or archives.

4 On the contrary, Art. 3(1) ODD states as a general principle that Member States must ensure that documents falling within the Directive's scope "shall be re-usable".

3.2.2 General conditions for re-use

The DGA solely defines certain basic principles (e.g., Art. 4) as a minimum set of conditions for the re-use by third parties which take into account the sensitivity of the data in scope (Art. 5), the possibility to charge fees (Art. 6), as well as certain procedural guideposts for handling requests for re-use (Arts. 8 and 9). Moreover, Member States must designate a competent body (with technical expertise) to assist public sector bodies in handling re-use requests (Art. 7).

First and foremost, the DGA prohibits exclusive arrangements for the re-use of data in order to avoid an exclusionary competitive advantage. An exclusive right to re-use can only be granted under rather strict conditions (necessary for products or services in the general interest that would otherwise not be possible, Art. 4(2)) and for a limited period of time (12 months, Art. 4(4)). In order to guarantee transparency, the decision to grant an exclusive arrangement has to be made available publicly (Art. 4(6)).

Most importantly, Art. 5(2) obliges public sector bodies to allow the re-use of data falling within the scope of the DGA under non-discriminatory, transparent, proportionate, and objectively justified conditions. Consequently, public sector bodies are, for instance, not allowed to impose conditions on data users which make the re-use unduly or even prohibitively difficult. Public sector bodies are allowed to charge a fee for making data available for re-use (Art. 6). In particular, Art. 6(4) allows for a layered scheme, charging less for small and medium-sized enterprises (SMEs) or research institutions. The charged fee must be based on the costs for making the data available (Art. 6(5)).

3.2.3 Additional safeguards

Since the DGA addresses *protected data*, the public sector body has the general obligation to ensure that the protected nature of data to be made available for re-use is preserved (Art. 5(3)).

In terms of personal data, the competent public sector body must therefore anonymise such data before making them available for re-use (Art. 5(3)(a)(i), Recital 15). In this case, the data no longer qualifies as personal data, meaning the GDPR does not apply. As an additional safeguard, Art. 5(5) DGA prohibits re-identifying natural persons and obliges data re-users to implement technical and organisational measures to prevent such re-identi-

fication. In case anonymised data is not suitable for the needs of the re-user, personal data can only be made available for re-use under additional requirements. In that case, all requirements for the lawful processing of personal data according to the GDPR would have to be met. In particular, the DGA itself does not constitute a legal basis for making personal data available for re-use (cf. Art. 5(6)). Moreover, the re-use of personal data should only occur via a "secure processing environment" provided by the public sector body, either remotely or on premise (see Recital 15, cf. Art. 5(3) (b), (c), (4)). Such secure processing environments are already used on a national and European level, such as by statistical offices.[5]

Art. 5 DGA also lays down further conditions for making confidential data (e.g., data protected as trade secret) or data subject to IP rights of third parties available for re-use. In general, data can be confidential for different reasons, stemming either from public[6] or private law. From the perspective of the latter, the protection of data as trade secrets according to the Trade Secrets Directive (2016/943) is the most relevant. Before making confidential data available for re-use, the public sector body should modify the data in a way that prevents the disclosure of confidential information (Art. 5(3) (a) (ii), Recital 15). As an additional preventive measure, the data re-user should be bound by means of a confidentiality agreement in case confidential information is discovered throughout the re-use despite the implemented safeguards (Art. 5(5)). Where a respective modification of the data is not possible or is not suitable for the intended re-use, confidential data can solely be made available when the right holder agrees ((Art. 5(6), (8)) or where such disclosure is lawful by virtue of EU or national law based on other grounds (Recital 18). In this case, the re-use should again occur via a "secure processing" environment, as mentioned above.

Data as such is not protected by IP rights (see Leistner and Antoine, 2022, p. 46). However, data collections can generally qualify as databases and be protected by copyright (Art. 3 et seqq. Database Directive (96/9/EC)) and/or the database sui-generis right (Art. 7 Database Directive). However, as copyright protection requires an original and creative selection or arrangement of the data, copyright protection will apply solely in rather exceptional cases, such as when a database is characterised by a highly unique structure. While in the case of confidential information already disclosing respective data qualifies as a relevant use act from trade secrets

5 See, for example, Eurostat (no date).
6 See, for example, statistic confidentiality according to Art. 338(2) TFEU.

perspective, IP protection comes into play for the question of whether a protected database can be re-used. If a database qualifies for protection, the DGA leaves the right holder's position arising from copyright or the sui-generis right untouched. Thus, it would have to be assessed under the Database Directive as to whether the use of the database by a re-user is lawful (see Art. 5(7) DGA).

On principle, public sector bodies can also qualify as right holders of the database through the sui-generis right. However, public sector bodies cannot invoke sui-generis protection in order to prevent the re-use of the requested data (see Art. 5(7) DGA); rather they should exercise their right only in a way that facilitates re-use (Recital 17 DGA).

3.2.4 Safeguards for the transfer of non-personal data to third countries

As an additional measure, even non-personal data that is confidential or subject to IP rights can solely be transferred to third countries outside the EU when appropriate safeguards are implemented.[7] These provisions are, to a certain extent, inspired by the GDPR's rules on the transfer of personal data to third countries. First of all, the re-user must inform the public sector body when requesting data for re-use about the intended data transmission to a third country, as well as the purposes of the requested re-use (Art. 5(9) DGA). In order to facilitate international data flows, the EC is empowered to adapt "equivalency decisions" – similar to the adequacy decisions of the GDPR – in order to *certify* that a third country meets similar standards for the protection of trade secrets and IP rights (Art. 5(12) DGA).

Where the requested confidential or IP-protected data should be transmitted to a country for which such decision of the EC does not exist, the re-user must contractually agree to use these data solely in accordance with EU law and to accept the jurisdiction of the courts or tribunals of the EU Member States for any dispute relating to the latter (Art. 5(10) DGA). According to Art. 5(13) DGA, future EU legislation can identify certain particularly sensitive categories of non-personal data which cannot be transmitted to third countries at all. The Regulation on the European

7 In the exceptional case that personal data should be made available for re-use, first and foremost, the requirements set forth in Art. 44 et seqq. GDPR for the transfer of personal data to third countries would have to be met.

Health Data Space (EHDS) already contains a respective provision for health data in its Art. 88.[8]

3.2.5 Transparent and effective framework for re-use requests

In order to practically facilitate the re-use of the data categories covered by the DGA, Member States must establish a "single information point" (SIP) (Art. 8). Aiming at providing a one-stop shop for re-use requests, these SIPs should provide an asset list containing an overview of all available data resources accompanied by relevant information describing the available data (Art. 8(2)). Member States are free to empower one competent body as central "intermediary" that directly handles and grants re-use requests (Art. 7(2)).

The competent public sector bodies must make the conditions for re-use and the procedure for requests available via the SIP (Art. 5 (1)). Based on the provided information, interested data users should then be able to send a request for the re-use of data via the SIP, which is then transmitted to the competent public sector body deciding about granting or refusing the request (Art. 8 (2)). On a European level, the EC has already established the European Single Access Point (ESAP) (Art. 8(4) DGA),[9] which merges the information provided by the national SIPs.

According to Art. 9, public sector bodies have to decide to grant or reject a request within a time frame of two months from the date of receiving the re-use request (Art. 9(1)). An extension of 30 days is possible in cases of exceptionally extensive and complex requests. Art. 9(2) grants the requesting person a right to seek redress, meaning that the decision taken by the public sector body can be challenged before the competent national authority or court.

3.2.6 Summary, guiding principles and perspective

Chapter II of the DGA aims at *unlocking* data held by the public sector that cannot be made available as *open data* under the ODD due to their sensi-

8 For more information about the EHDS, see Chapter 15 'The European Health Data Space: The Next Step in Data Regulation' by Lisa Markschies.

9 The ESAP is integrated to the European Data Portal "data.europa.eu" (European Union, no date). However, for the time being, only datasets from the Dutch and Czech National Single Information Points are available (as of 30 June 2024).

tive nature. By establishing a procedural framework for re-use requests and defining conditions for re-use that protect the data's particular character, the DGA aims to increase transparency. For potential re-users, the DGA's provisions clarify how access to respective data can be obtained and under which conditions, as well as which limitations must be respected during re-use (e.g., from a technical perspective). For actors who might have a legal position in the data at stake, the DGA's framework guarantees that these positions (i.e., in terms of the sensitivity of the data) are respected. From a public interest perspective, the standardised procedural mechanism for re-use requests and the transparent and *fair* conditions for re-use do not only facilitate the re-use of data held by the public sector in practice, but also increase trust in public institutions. Public sector bodies obtaining data as part of their public tasks are responsible for protecting respective data even when making them available to third parties for re-use. Moreover, they should, at the same time, contribute to research and innovation in the general interest by allowing re-use. This aspect is, for instance, materialised in the *research-friendly* approach explicitly followed by the DGA (Recitals 15 and 16). Consequently, in terms of scientific research, data should be *as open as possible, as closed as necessary*. However, practically speaking, it is worth bearing in mind that the DGA does not contain any obligation for making data available for re-use. Rather, the Member States have ample discretion in deciding which data categories should be accessible for re-use under national law and under which conditions.

3.3 Data intermediaries: the emerge of neutral and trustworthy players?

The second set of provisions contained in the DGA does not address public institutions, but rather aims to establish reliable and trustworthy data intermediaries in the markets that contribute to facilitating data flows between individuals and businesses, as well as in relation to the public sector. Enhancing data access and fostering data sharing faces a number of legal, organisational, and technical challenges – particularly in terms of making the desired data flows work in practice. Consequently, data intermediaries have been identified as (potential) key enablers for facilitating data access and data sharing (Recital 27). High hopes have been placed on these actors, with a real "data intermediary hype" (Richter, 2023, p. 458) having been observed in recent years.

In order to foster the development of data intermediaries in the European single market, the DGA introduces a mandatory legal framework for providing data intermediation services in general and data altruism organisations in particular. The underlying idea is that implementing a set of rules to which providers of respective services must comply will increase trust in these players. Natural and legal persons should thereby be encouraged to make use of data intermediaries offering a trusted and secure environment for data exchange and sharing (Hennemann and von Ditfurth, 2022, p. 1907). In particular, the European data intermediaries are meant to form a counterpart to the internationally dominating platforms with their immense market and data power (Recital 32 DGA; European Commission, 2020b, p. 16; Richter, 2023, p. 462). By introducing public registers and a *certification* scheme with labels and logos, compliance with DGA-defined rules should be clearly signalled.

3.3.1 Data intermediation services (Chapter III)

Chapter III of the DGA addresses data intermediation services. As an umbrella term, data intermediation service describes a very heterogenous concept. Diverse studies and research papers on a possible categorisation and classification of different data intermediaries have been published in recent years, taking into account various perspectives and disciplines (see Richter and Slowinski, 2019, p. 10; OECD, 2019, p. 36; Wernick, Olk and von Grafenstein, 2020, p. 67; Simon et al., 2020, p. 20; Micheli et al., 2023; Schneider, 2023, 2024).

However, all data intermediaries share two basic features in common: first, their role as neutral, independent third parties; and, second, their function to bring together a person having data and a person interested in this data, as well as to facilitate the respective data flow between these two parties (cf. Recital 27 DGA; Richter and Slowinski, 2019, p. 13; Richter, 2023, p. 459). Notwithstanding, the realisation and organisation of an intermediation service can vary widely (see Recital 27 DGA). As such, the DGA's definition of data intermediation service covers a broad range of services with different purposes and very different forms of organisation.

In line with the overall objective to create neutral and trustworthy data intermediation services, the DGA introduces a notification process and defines specific conditions under which respective services have to be provided.

3.3.2 Definition of data intermediation service

Following these two main characteristics that data intermediaries share, the DGA's definition of "data intermediation service" (Art. 2(11) DGA) adds two additional and, at the same time, limiting features (Richter, 2023, p. 462): first, the purpose of establishing a commercial relationship between data holder and data user; and, second, the open nature of the service ("undetermined number of data holders and users"). Thus, neither services establishing non-commercial relationships between data holders and users (e.g., open access repositories for research data, see Recital 29 DGA), nor closed networks qualify as data intermediation services in the sense of the DGA. Possible examples of data intermediation services are, for instance, data marketplaces or platforms, data pools open to all interested parties, and providers of "data sharing ecosystems", such as the envisaged common European data spaces (Recital 28 DGA). This has particular relevance, as providers of common European data spaces might therefore have to fulfil – in particular circumstances – the obligations outlined in Arts. 11 and 12 of the DGA.

Data intermediation services can cover both personal and non-personal data (European Commission, 2020b, p. 5). Therefore, services particularly tailored to personal data – often called Personal Information Management Systems (PIMS) – that provide, for instance, tools for managing consent to the processing of personal data and for exercising the data subject's right, as foreseen in the GDPR (Recital 30 DGA), also qualify as data intermediation services. However, in terms of processing personal data, the GDPR always fully applies.

The provision of mere technical means for data sharing (e.g., in the form of cloud storage, software tools) does not qualify as a data intermediation service. Moreover, services that aggregate, enrich, or transform data for the purpose of adding substantial value, intermediation services for copyright-protected content (i.e., online content-sharing service pursuant to the DSM Directive), and data sharing services offered by the public sector which are not aimed at establishing commercial relationships[10] do not constitute data intermediation services either (see Art. 2(11) DGA).

10 On principle, public sector bodies can also act as intermediation services (Recital 27 DGA); however, only when aiming at the establishment of commercial relationships do they fall under the definition in Art. 2(11). Public sector bodies making data

3.3.3 Notification process and public register

Before beginning their activities, providers of a data intermediation service have to submit a notification to the national competent authority (Art. 11(1), (4) DGA), designated by Member States (Arts. 13, 14 DGA). According to Art. 10, the notification process is mandatory for (a) providers of platforms or comparable infrastructure services allowing bilateral or multilateral connections and data exchanges between data holders and potential data users (e.g., data sharing platforms or marketplaces where businesses can exchange data); (b) PIMS allowing data subjects to make personal data available and to exercise their rights contained in the GDPR (e.g., PIMS or data wallets, which allow individuals to control their personal data); and (c) data cooperatives,[11] where users are proper members of the structure (such as health data cooperatives, where patients can share their health data for research purposes).

The notification has to contain basic information, such as the name, legal status, form, ownership structure, relevant subsidiaries, number of national registers, address of the main establishment or the legal representative, public website, contact details of a competent contact person, and the description of the offered services (Art. 11(6) DGA). Data intermediation service providers in this sense must comply with the obligations set out in Art. 11 by 24 September 2025 (Art. 37 DGA). After having received the notification, the competent authority issues a declaration, confirming that the data intermediation services provider has submitted a notification containing all relevant information pursuant to Art. 11(6) (Art. 11(8)). In addition, the data intermediation service can request the competent authority to confirm its compliance with all obligations defined in Arts. 11 and 12 (Art. 11(9)). The national competent authorities report any notification to the EU, which, in turn, provides a public register of recognised data intermediaries (Art. 11(10)).[12] Where the competent authority issues a respective confirmation, the data intermediation service is further allowed to use the label "data intermediation services provider recognised in the Union" and the following logo:

available for re-use pursuant to Chapter II do not qualify as intermediation service in this sense (Recital 28).

11 See the definition in Art. 2(15) with Recital 31, and, on data cooperatives, Zingales (2022, p. 8).

12 The register is available at European Commission (2024).

Figure 1: Common logo as adopted through Commission Implementing Regulation (EU) 2023/1622 of 9 August 2023 on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union

3.3.4 Conditions for providing data intermediation services

In order to guarantee the envisaged role of a data intermediation service as a neutral and trustworthy third party, Art. 12 DGA defines mandatory conditions under which data intermediation services have to be provided.

Due to the strict neutrality principle (see also Recital 33; Spindler, 2021, p. 107; Baloup et al, 2021, p. 31), the DGA, first and foremost, mandates that data intermediation services have to be provided as structurally separate from other services, meaning by a separate legal person (Art. 12 (a)). According to Recital 32, "data intermediation services providers should offer a novel, 'European' way of data governance, by providing a separation in the data economy between data provision, intermediation and use". Notwithstanding, such structural separation, i.e., in the form of a separate legal person (Rec. 33), has a far-reaching economic impact that might even disincentivise the development of data intermediation services (see Richter, 2023, p. 465; Hartl and Ludin, 2021, p. 537).

Second, Art. 12 DGA additionally limits the purposes for which intermediation services can use data. Most importantly, providers are obliged to not use data for purposes other than the provision of a data intermediation service (Art. 12 (a)). Moreover, they may not use data stemming from users' activities for other purposes than the development of the intermediation service (Art. 12 (c)), and not change the data format unless this is requested by the user or necessary for enhancing interoperability or mandated by law (Art. 12 (d)). Additional tools and services can only be offered for the specific purpose of facilitating the exchange of data (Art. 12 (e), Recital 32). Indeed, accepting such an offer would require an explicit request or approval of the data subject or data holder. In sum, the purpose limitations seek to prevent conflicts of interest and to *unbundle* services (Richter, 2022, p. 463) in the interest of the user.

Third, Art. 12 further specifies the conditions under which the data intermediation service has to be offered. According to Art. 12 (b), the intermediation service (including the pricing) must not be tied to other services. Furthermore, access to the data intermediation service has to be granted under fair, transparent, and non-discriminatory conditions for both data holders, data subjects, and users. Even in the case of insolvency, data intermediation service providers have to ensure that data holders and users are able to access and retrieve their data (Art. 12 (h)).

Fourth, providers of data intermediation services are obliged to implement technical and organisational measures for preventing fraudulent or abusive practices (Art. 12 (g)), safeguard a reasonable continuity of service in case of insolvency (Art. 12 (h)), and prevent unlawful access to non-personal data (Art. 12 (j)). They have to inform data holders in case of unauthorised data access (Art. 12 (k)), comply with IT-security standards for storage, processing and transmission of data (Art. 12 (l)), and maintain log records of the data intermediation activity (Art. 12 (o)). Moreover, data intermediation services should explicitly contribute to enhancing interoperability, also in terms of other intermediation services (Art. 12 (d), (i)).

As regards personal data, Art. 12 (m) adds an additional layer of responsibility for data intermediation service providers: they must act in data subjects' best interests, inter alia by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible, and easily accessible manner. According to Recital 30, this could include advising data subjects on the possible use of data, conducting due diligence checks on data users before allowing access to personal data, or offering a technical solution for in-situ access to personal data instead of transferring it to third parties. Thus, Art. 12 (m) does not contain a clear-cut set of measures that data intermediation services must implement for this purpose. This leaves providers with a wide discretion on the one hand, but also carries significant legal uncertainty on the other. In particular, the abstract obligation to act in the data subjects' best interest is – pursuant to Recital 33 – understood as an intermediation service's "fiduciary duty" towards the individual. Consequently, Art. 12 (m) imposes a far-reaching responsibility on personal data-related intermediation services far exceeding the strict neutrality principle (less critical e.g., Specht-Riemenschneider in Specht-Riemenschneider & Hennemann, 2023, Art. 12 para. 98 arguing that the structural imbalance of power to the detriment of data subjects justifies such fiduciary duty).

3.3.5 Summary, guiding principles, and perspective

The obligations contained in Chapter III aim to safeguard the strict neutrality of data intermediation services. Most importantly, respective services have to be provided as structurally separate from other services. In addition, providers must not use the data "consigned" to them for their own purposes and additional services can only be offered to the user under certain circumstances. All of these obligations form the prerequisites for distinguishing the *European way* of data intermediation services (Recital 32) from data leeches. The framework outlined for the provision of data intermediation services is thus, on principle, suitable for increasing trust in the respective services as potential users do not have to fear that "their" data is being used for the provider's own interests. As such, the strict conditions under which data intermediation services can be provided could, on principle, incentivise data holders and potential data users to make use of these respective services.

However, it remains to be seen whether there are sufficient incentives for data intermediation services to generate their respective business models. The obligations to which data intermediation services providers must comply under the DGA are quite far-reaching. Offering data intermediation services in accordance with the DGA's framework has a cost side. Even already existing intermediaries are still in their "infancy" (Gellert and Graef, 2021, p. 11), or in a "rather nascent phase" (Richter, 2023, p. 460). In this context, it has also to be kept in mind that no ex-ante examination by the competent authority is conducted on a substantive level. Thus, data intermediation services must assess their compliance on their own account, but at the same time face ex-post supervision by the national competent authority. Although this mechanism has been introduced with the idea to limit both the regulatory burden and the service providers' costs (Gellert and Graef, 2021, p. 9), it may result in a model that tends to be rather unattractive for the relevant players (Hartl and Ludin, 2021, p. 537). On principle, being able to use the label of recognised data intermediation service could set certain incentives for providers as it signals their compliance with the DGA to the market, and thus their nature as a neutral and trustworthy third party. However, this would require that potential users of data intermediation services sufficiently value the trustworthiness of such a service when taking decisions and that increased trust can really incentivise data sharing via respective services (further discussed in Section 4.). Therefore, it remains to be seen whether the framework provided by

the DGA helps data intermediation services scale up, or rather stifles the development of respective business models. However, at least eight data intermediation services from Finland, France, and Hungary are currently registered in the EU (European Commission, 2024b).

3.3.6 Data altruism organisations (Chapter IV)

For the particular category of data altruism organisations – put simply, data intermediaries acting not-for-profit and for the social good – Art. 16 et seqq. DGA provide specific provisions. As mentioned above, the obligations for data intermediation services do not explicitly apply to data altruism organisations (Art. 15).

As can data intermediation services, data altruism organisations can appear in multiple forms. The basic constellation the DGA seems to have in mind are data altruism organisations that, in a first step, pool data for a particular purpose of general interest, and, in a second step, allow access to this data (e.g., for research purposes). An illustrative – and often-quoted – example here is Germany's "Corona Data Donation App" (Corona Datenspende, 2024). During the COVID-19 pandemic, users were able to share such data as resting pulse, daily activity, and sleep duration via a smartphone app. Over half a million people in Germany decided to support the project and donated their data. The data was then used for scientific research on the long-term effects of the COVID-19 virus. However, the DGA also seems to cover constellations in which data altruism organisations primarily provide tools allowing data subjects or data holders to easily give consent (personal data) or permission (non-personal data) to the data processing of third parties (cf. Art. 21(6)). Thus, data wallets or consent management tools can also qualify as data altruism organisations, at least as far as they pursue objectives of general interest or act for the social good.

When organisations conduct data altruism activities, they can apply for registration in the public register what requires to fulfil further pre-requisites when providing their service. This also entails the obligation to introduce tools allowing the donating data subject or data holder to manage consent and permission.

3.3.7 Definition of data altruism

The definition of data altruism contained in Art. 2(16) of the DGA is characterised by three main features: (1) data subjects or data holders deliberately share "their" data with a data altruism organisation by means of giving consent or permission to the use of the respective data; (2) data altruism organisations have to work on a not-for-profit basis and are only allowed to seek compensation for covering the costs incurred from making their data available; and (3) data is made available for the social good, i.e., for objectives of general interest. Regarding objectives of general interest, Recital 35 lists possible examples, such as "healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, or public policy making".

3.3.8 Registration process and public register

Compared to data intermediation services, which are subject to a mandatory *notification* process, data altruism organisations can be *registered* voluntarily with the competent national authority. In this regard, data altruism organisations need to apply for registration (Art. 19(4) DGA) and, as a prerequisite, must meet the requirements set forth in Art. 18. The competent authority only registers a data altruism organisation if it complies with the respective obligations (Art. 19(5)). Thus, the competent authority not only examines the application for registration formally, but also substantively. Moreover, the competent authorities – which the Member States have to designate (Art. 23) – monitor and supervise the compliance of data altruism organisations after registration (Art. 24).

Art. 18 defines the requirements for registration. This provision both specifies the notion of data altruism organisation and adds further criteria to be fulfilled in order to qualify for registration. Comparable to the provisions on data intermediation services in general, these requirements aim at guaranteeing the neutrality of data altruism organisations. However, the criteria set forth for data altruism organisations are even stricter in this regard. This reflects the particular altruistic character of respective organisations, distinguishing them from "normal" data intermediaries. As such, apart from making their data available for objectives of general interest, data altruism organisations must also be structured as an (independent)

legal person. Further, a data altruism organisation does not only have to operate on a not-for-profit basis, but it has to be legally independent from any entity operating on a for-profit basis. Moreover, data altruism activities must be conducted through a structure that is functionally separate from other activities.

In addition, data altruism organisations must comply with the rulebook developed by the EC according to Art. 22 DGA. However, so far, this rulebook does not exist. Once registered, a data altruism organisation is allowed to use the label data altruism organisation recognised in the Union as well as the respective logo:

Figure 2: Common logo as adopted through Commission Implementing Regulation (EU) 2023/1622 of 9 August 2023 on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union

The Member States must establish a national register of recognised data altruism organisations (RDAOs); the latter of which must then be reported to the EC, who will then compile the information in the EU register of RDAOs (Art. 17 DGA; see European Commission, 2024c). Currently, only one data altruism organisation is registered,[13] the "Associació Dades pel Benestar Planetari (DATALOG)" from Spain. DATALOG operates in Barcelona and was developed from a project conducted by the Universitat Pompeu Fabra. DATALOG provides a platform where citizens can upload their invoices for consumption of public services, such as water, gas, and electricity. For the individual user, the platform not only allows a centralised management of respective invoices, but also an analysis of the individual consumption, thereby allowing for its further optimisation in a responsible and sustainable manner. As regards the city of Barcelona, consumption data can be mapped and aggregated on a large scale. Data analysis can then show tendencies, patterns, and correlations regarding

13 As of 2 July 2024.

citizens' consumption, thereby enabling smarter and more sustainable decisions for the city's further development.

3.3.9 Further obligations for recognised data altruism organisations

The DGA does not stop at defining registration requirements, but also outlines certain transparency duties (Art. 20) and conditions under which the RDAOs must conduct their activities (Art. 21).

In order to make the work of data altruism organisations transparent, RDAOs are obliged to keep full and accurate records on which natural or legal persons were given the possibility to process data held by the RDAO, when or for how long such processing took place, what the purpose of processing was, and whether a fee was paid (Art. 20(1)). Furthermore, RDAOs have to submit an annual activity report to the competent authority (Art. 20(2)).

Regarding the data-sharing process, the RDAO must inform the data subject or holder before sharing any data, in a clear and easily comprehensible manner, for which objectives of general interest the RDAO will conduct data processing activities (Art. 21(1) (a)). Where personal data is concerned, the information needs to be more specific, demonstrating a "specified, explicit and legitimate purpose" for which personal data is processed. RDAOs must not use the data provided to them for other purposes than the objectives of general interest (Art. 21(2)). Where data processing activities are conducted in third countries outside the EU or where data might be made available in such countries, the RDAO has to provide further information (Art. 21(1) (b), (6)).

Regarding the data processing activities, the RDAO must ensure an appropriate level of security for data storage and processing (Art. 21(4)) – also with regard to non-personal data – and to inform data holders of any unauthorised transfer, access, or use of non-personal data (Art. 21(5)). Where (also) personal data is at stake, the provisions of the GDPR take precedence.

3.3.10 Consent and permission

In order to facilitate data sharing for the social good in practice, RDAOs should provide tools for easily providing and withdrawing consent (person-

al data) and permission (non-personal data) (Art. 21(3) DGA). However, this is no easy task. Obtaining valid consent for the processing of personal data under the GDPR (Art. 6(1) (a) GDPR) is subject to certain requirements that, particularly where the purpose of the processing is not clear from the outset, are difficult to fulfil. This is also the case when data is collected and made available for altruistic grounds by RDAOs (cf. Recital 50 DGA; Specht-Riemenschneider, 2023, p. 658; von Hagen and Völzmann, 2022, p. 177). Thus, obtaining consent pursuant to Art. 6(1) (a) GDPR and – for very sensitive data, such as health data – and under the even stricter requirements of Art. 9(1) (a) GDPR, has been identified as a major obstacle and challenge to data altruism activities and scientific research in general (cf. Steinrötter, 2021, p. 61). In order to *help* data altruism organisations deal with this issue, the EC will, according to Art. 25 DGA, develop a European data altruism consent form. However, this has yet to be adopted. In addition, it still remains to be seen how helpful the final consent form will be (see Schreiber, Pommerening and Schoel, para. 88). First, the European Data Protection Board has been consistently hesitant to approve a model consent form as fulfilling the requirements set forth in the GDPR, arguing that it depends on the particular circumstances of any single case. Hence, it is unlikely that a consent form will be adopted which could be used straightforwardly (Rachut, 2024, p.252). Second, a technical solution for obtaining (and withdrawing) consent in line with the GDPR would be most favourable for making data wallets, consent management tools, and other data sharing platforms work in practice (European Commission, 2020b, p. 14). Whether guidelines on how such technical implementation could look like will (and can) be developed is currently an open question.

An additional layer of complexity is introduced by the unclear legal nature of the permission a data holder has to give for the processing of non-personal data. As far as non-personal data is not a trade secret and a data collection is not protected by IP rights, no exclusive position in relation to non-personal data exists. Consequently, a permission to use non-personal data would actually not be necessary. Most likely, the required permission has to be interpreted as the very basic (implicit) agreement between the RDAO and the data holder sharing non-personal data on the provision of the data altruism service. Notwithstanding, the wording of Art. 25 DGA suggests that the European Consent Form will also contain a template for giving permission to the processing of non-personal data.

3.3.11 Summary, guiding principles, and perspective

In principle, the provisions on data altruism organisations rightly address three main obstacles to data sharing for the social good which have been identified in recent years: no established players in the markets, a lack of trust, and legal uncertainty (particularly regarding the processing of personal data).

However, the requirements that data altruism organisations have to meet in order to be registered are high. From the very outset, the need to be established as a legal person excludes all kinds of projects and studies which are, however, the most common form of organisation in scientific research (Spindler, 2021, p. 105). As data altruism organisations must operate on a not-for-profit basis and be legally independent from any entity operating on a for-profit basis, they will need financial resources to be able to run their services (in terms of research data repositories, see OECD, 2017, p. 20). Moreover, they must provide their service as functionally separate from any other service; this requires building an independent organisational and technical infrastructure which goes hand in hand with significant costs. Whether sufficient data altruism organisations fulfilling these requirements will appear must be awaited. Pessimistically speaking, the mere number of only *one* registered data altruism organisation throughout 27 Member States raises certain doubts in this regard.

In terms of the second point, trust, the DGA's strict requirements are suitable for safeguarding the envisaged role of RDAOs as not only neutral, but also altruistic players. Due to the particular character of RDAOs acting for the social good, it is convincing to define even stricter requirements than for other types of data intermediaries. Potential data donors should be sure that "their" data is only used for the purposes in the general interest they wished them to be used for, such as for health research. Thus, also in terms of data altruism organisations, the DGA can contribute to increased trust in respective players. Apart from the question of whether data altruism organisations will emerge in the EU despite the strict requirements set out in the DGA, the question also arises as to whether the trustworthiness of RDAOs is sufficient to incentivise data subjects and data holders to donate data for objectives of general interest. Whether potential data donors can be prompted to share data by offering additional incentives, such as by providing small rewards to persons who donate their data, remains open. Recital 45 DGA solely states that "data subjects should be able to receive

compensation related only to the costs they incur when making their data available".

Notwithstanding, if, third, the existing legal uncertainty on how to obtain valid consent for pooling and making personal data available for altruistic purposes in line with the GDPR cannot be reduced, it may be difficult in practice to make these initiatives fly.

From a practical point of view, the EHDS[14] may significantly impact the role of data altruism organisations. So far, data cooperatives and comparable projects for data donation have primarily existed in the health sector. With the new rules on the secondary use of health data, the relevance of data altruism organisations in the health sector might decrease. As the example of Spain's DATALOG shows, sustainability and green development might currently be the most promising sector for the development of data altruism organisations.

4. The role of trust in business and consumer decisions?

As the analysis has shown, the DGA is heavily reliant on the principle of trust. This concerns both the set of rules on a standardised mechanism for facilitating the re-use of data held by public sector bodies that cannot be made available as open data due to their sensitivity and the provisions on data intermediaries. As shown above (see Section 2), from a theoretical point of view, legal norms can reduce complexity, as the uncertainty over a counterpart's behaviour is perceived as being narrowed down from a multitude of possible options to fewer probable – lawful – options. This reduces risk and, thus, can increase trust. Hence, the DGA's provisions on G2B data sharing and data intermediaries are well suited to the theoretical concept of trust, both from a sociological and a legal perspective. However, the follow-up question arises as to whether this concept works in practice and, in particular, whether the relevant market players really value trust when taking business and consumer decisions.

Through establishing a minimum set of rules for facilitating data re-use requests and defining conditions for re-use that aim to protect the data's sensitive character, the DGA pursues the objective of increasing transparency. A higher degree of transparency can increase citizens' trust in public

14 For more information on the EHDS, see Chapter 15 'The European Health Data Space: The Next Step in Data Regulation' by Lisa Markschies.

sector bodies. On the one hand, public sector bodies should not be able to retain data that are valuable for scientific research or innovative business models, while, on the other hand, they are bound to their public task of preserving the data's sensitive nature, even when making them available for re-use. Hence, this framework can contribute to a more transparent mechanism that might favour trust in the acting institutions (i.e., public sector bodies). Notwithstanding, the success of the framework for G2B data flows beyond open data will heavily depend on whether data access and re-use requests are handled efficiently in practice and – most importantly – which data the Member States decide to make available. Thus, the concept of trust plays an important role in this context, but is, on its own, not decisive for the success of the DGA's objectives and the envisaged decisions of the involved actors. When looking at the provisions on data intermediaries, trust, however, serves as the central reference point. In the DGA, the European legislator follows the assumption that a lack of trust has, thus far, prevented data intermediaries from emerging. However, no empirical evidence exists in this regard (Hennemann and von Ditfurth, 2022, p. 1910; Kerber, 2021, p. 3).

First, the question arises whether a mandatory legal framework for data intermediaries as provided by the DGA can – as such – increase trust in these players. Taking into account the findings presented above, from a theoretical point of view, such a legal framework is indeed suitable for reducing the (perception of) risk that data intermediaries might opt to act in such a way as to serve their own business interests – as the big platforms mostly do. Consequently, the framework introduced by the DGA indeed has the potential to increase users' trust in data intermediaries. Increased trust might therefore impact users' choices.

Second, users would not only have to trust these players, but also have confidence in the business model of trustworthy intermediaries as such. In short, users would have to be willing to use data intermediary services for managing or sharing data. Third, even if that were the case, users, would have to sufficiently value *trust* when taking (privacy-related) decisions (Kerber, 2021, p. 4; Waldman, 2018, p. 47). From a theoretical point of view, trust seems to be the main *topos* for deciding with whom data should be shared. This is all the more true for the case of data, since data holders and data subjects, to a certain extent, lose *control* over data when having made them available to a third party for the first time. Notwithstanding, what drives user's privacy decisions has not for nothing been a highly debated question for decades – particularly from the perspective of behavioural economics, respectively law

and economics (see inter alia (influentially) Acquisti and Grossklags, 2005); for a recent empirical study, see Sprigman and Tontrup, 2024, p. 11, with comprehensive references on previous research). Consumer and business decisions are based on multiple factors and complex relations. For instance, the DGA also introduces logos and labels that should clearly signal compliance with the rules defined therein in order to provide transparent and easily accessible information. However, ultimately, consumer and business choices might not be rational, even when it comes down to trust. In addition, the price, certain network effects, and the straightforwardness of a service seem to be decisive factors for driving user decisions – being a *data leech* or recognised *data intermediary* that receives the data (Gellert and Graef, 2021, p. 8; Sprigman and Tontrup, 2024, p. 7).

Thus, although the objectives followed by the DGA theoretically align with the academic concept of trust, from a practical point of view, it seems questionable whether trust sufficiently influences business or consumer decisions, particularly in the data and platform economy. However (and more positively), from interdisciplinary perspective, this offers a plethora of anchoring points for further empirical research which would be necessary for answering these questions comprehensively.

5. Concluding remarks

The DGA is built on the assumption that increased trust can significantly influence user choices, thereby contributing to the overall objective to foster and facilitate data sharing in the EU. The idea that a clear legal framework, being for G2B data flows and for the provision of intermediation services, has the potential to strengthen trust in the respective actors and institutions and can thus impact users' decisions fits perfectly into the theoretical concept of trust. However, practically speaking, the question remains whether trust, on its own, can assume the envisaged essential role for consumer or business decisions in this regard.

All in all, therefore, it seems particularly doubtful that data intermediaries can fulfil the immense expectations that have been projected on them. In principle, data intermediaries could indeed assume an important role in the data economy, such as by facilitating voluntary data sharing and exchange, providing the infrastructure for making mandatory access regimes work in practice or offering tools for enforcing data subject's rights and managing consent for the processing of personal data in line with the

GDPR (Specht-Riemenschneider and Kerber, 2022, p. 24). However, the requirements are rather high and, for the time being, it seems questionable whether sufficient intermediaries fulfilling the respective standards will appear in the markets. This is, first, due to the cost side of the measures the DGA implements. Second, incentives for generating respective data intermediation services seem to be lacking, as it remains unclear whether users will turn to data intermediation services as expected.

Whether the DGA will positively impact the re-use of data held by public sector bodies does not solely depend on trust. Rather, which data the Member States decide to make available, and under which conditions, will be decisive. Hence, although the concept of trust also shapes the DGA's provisions on the re-use of public sector bodies, trust, on its own, is not decisive for the success of the DGA's objectives and the envisaged decisions of the involved actors.

Considering the broader picture, the EU is following a strong regulatory approach in trying to promote innovation in line with such democratic values as freedom of choice and digital sovereignty, safety and security, participation, and sustainability. In so doing, the EU is seeking to promote *regulation* as a unique selling point on a global level. This rationale underlies many of the recent EU legislative acts on data and the digital environment, and also shapes the DGA's provisions on data intermediaries. The DGA once more is an expression of a strongly *mission-based* legal intervention – a phenomenon which characterises European data-related legislation significantly and aims at shaping markets. Whether the relevant players will follow this approach remains to be seen.

References

Acquisti, A. and Grossklags, J. (2005) 'Privacy and rationality in individual decision making', *IEEE Security & Privacy*, 3(1), pp. 26–33.

Baloup, J., Bayamlioğlu, E., Benmayor, A et al (2021) 'White paper on the data governance act'. *SSRN* [Online]. Available at: https://ssrn.com/abstract=3872703 (Accessed: 27 January 2025).

Cole, M. (2022) 'Vertrauenswürdigkeit des Online-Umfelds', *UFITA*, pp. 305 – 327.

Corona Datenspende (2024) [Online]. Available at: https://corona-datenspende.github.io/en/ (Accessed: 27 January 2025).

'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')' (2000) *Official Journal* L 178, 17 July, pp. 1–16 [Online]. Available at: http://data.europa.eu/eli/dir/2000/31/oj (Accessed: 19 January 2025).

'Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' (2016) *Official Journal* L 157, 15 June, pp. 1–18 [Online]. Available at: http://data.europa.eu/eli/dir/2016/943/oj (Accessed: 27 January 2025).

'Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases' (1996) *Official Journal* L 77, 27 March, pp. 20–28 [Online]. Available at: http://data.europa.eu/eli/dir/1996/9/oj (Accessed: 27 January 2025).

European Commission (2018) *Commission staff working document guidance on sharing private sector data in the European data economy*. COM(2018) 232 final [Online]. Available at: https://digital-strategy.ec.europa.eu/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy (Accessed: 27 January 2025).

European Commission (2020a) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – a European strategy for data*. COM(2020) 66 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066 (Accessed: 27 January 2025).

European Commission (2020b) *Commission staff working document, impact assessment report, accompanying the document proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act).* SWD(2020) 295 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020SC0295 (Accessed: 27 January 2025).

European Commission (2024a), *Implementing the Data Governance Act – guidance document* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/new-practical-guide-data-governance-act (Accessed: 29 January 2025).

European Commission (2024b) *EU register of data intermediation services* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services (Accessed: 27 January 2025).

European Commission (2024c) *EU register of recognised data altruism organisations* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations (Accessed: 29 January 2025).

European Union (no date) *European data* [Online]. Available at: https://data.europa.eu/data/datasets?superCatalog=erpd&locale=en (Accessed: 27 January 2025).

Eurostat (no date) *Microdata.* [Online]. Available at: https://ec.europa.eu/eurostat/web/microdata (Accessed: 27 January 2025).

Gellert, R. and Graef, I. (2021) 'The European Commission's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing' *TILEC Discussion Paper No. DP2021-006. SSRN* [Online]. Available at: https://ssrn.com/abstract=3814721 (Accessed: 27 January 2025).

Hartl, A. and Ludin, A. (2021) 'Recht der Datenzugänge', *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung*, pp. 534–538.

Hennemann, M. and von Ditfurth, L. (2022) 'Datenintermediäre und Data Governance Act', *Neue Juristische Wochenschrift*, pp. 1905–1910.

Kaesling, K. (2022) 'Vertrauen als Topos der Regulierung vertrauenswürdiger Hinweisgeber im Digital Services Act', *UFITA*, pp. 328–351.

Kerber, W. (2021) *DGA – einige Bemerkungen aus ökonomischer Sicht*. University of Marburg [Online]. Available at: https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/pdf-dateien/kerber_dga_einige-bemerkungen_21012021.pdf (Accessed: 27 January 2025).

Lauber-Rönsberg (2022) '"Vertrauenswürdige Rechtsinhaber" im Kontext des Urheberrechts', *UFITA*, pp. 265–276.

Lauber-Rönsberg, A. and Becker, P. (2023) 'Auswirkungen des Data Governance Act auf Forschungseinrichtungen und Repositorien', *Recht und Zugang*, pp. 30–47.

Leistner, M. and Antoine, L. (2022) *IPR and the use of open data and data sharing initiatives by public and private actors*. European Parliament [Online]. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)732266 (Accessed: 27 January 2025).

Liesching, M. (2022) 'Hassrede und NetzDG – Vertrauenskonzepte im Beschwerde-Management', *UFITA*, pp. 252–264.

Luhmann, N. (2014) *Vertrauen*. 5th ed. Constance & Munich: UVK Verlagsgesellschaft mbH.

Micheli, M. et al. (2023) *Mapping the landscape of data intermediaries*. Publications Office of the European Union [Online]. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC133988 (Accessed: 27 January 2025).

OECD (2017) 'Business models for sustainable research data repositories', *OECD Science, Technology and Industry Policy Papers* 47 [Online]. Available at: https://doi.org/10.1787/302b12bb-en (Accessed: 27 January 2025).

OECD (2019) *Enhancing access to and sharing of data: reconciling risks and benefits for data re-use across societies*. OECD Publishing [Online]. Available at: https://doi.org/10.1787/276aaca8-en (Accessed: 27 January 2025).

OECD (2022a) 'Fostering cross-border data flows with trust', *OECD Digital Economy Papers, No. 343* [Online]. Available at: https://doi.org/10.1787/139b32ad-en (Accessed: 27 January 2025).

OECD (2022b) *Declaration on a trusted, sustainable and inclusive digital future*. OECD Legal Instruments [Online]. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488 (Accessed: 27 January 2025).

Oxford English Dictionary (2024) '*trust*' (*n.*). Oxford: Oxford University Press [Online]. Available at: https://doi.org/10.1093/OED/5777528687 (Accessed: 27 January 2025).

Peukert, A. (2022) 'Vertrauen als Topos der Plattformregulierung', *UFITA*, 8, pp. 230–251.

Peukert, A. (2023) 'The regulation of disinformation in the EU – overview and open questions' *SSRN* [Online]. Available at: https://ssrn.com/abstract=4496691 (Accessed: 27 January 2025).

Rachut, S. (2024) 'Datenaltruismus unter dem Data Governance Act. Verpasste Chance beim Zusammenspiel von DGA und DS-GVO', *Zeitschrift für Datenschutz*, 14(5), pp. 248–253.

'Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.' *Official Journal* L 186, 11 July pp. 57–79 [Online]. Available at: http://data.europa.eu/eli/reg/2019/1150/oj (Accessed: 27 January 2025).

'Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)' (2022) *Official Journal* L 152, 3 June, pp. 1–44, [Online]. Available at: http://data.europa.eu/eli/reg/2022/868/oj (Accessed: 27 January 2025).

'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (2024) *Official Journal* L, 2024/1689, 12 July [Online]. Available at: http://data.europa.eu/eli/reg/2024/1689/oj (Accessed: 27 January 2025).

'Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847' (2025) *Official Journal* L, 2025/327, 5 March 2025 [Online]. Available at: http://data.europa.eu/eli/reg/2025/327/oj (Accessed: 7 March 2025).

Richter, H. (2022) 'Ankunft im Post-Open-Data-Zeitalter', *Zeitschrift für Datenschutz,* 12(1), pp. 3–8.

Richter, H. (2023) 'Looking at the Data Governance Act and beyond: how to better integrate data intermediaries in the market order for data sharing', *GRUR International Journal of European and International IP Law*, 72(5), pp. 458–470.

Richter, H. and Slowinski, P. (2019) 'The data sharing economy: on the emergence of new intermediaries', *International Review of Intellectual Property and Competition Law*, 50, pp. 4–29.

Schneider, I. (2023) 'Digital sovereignty and governance in the data economy: data trusteeship instead of property rights on data' in Godt, C. and Lamping, M. (eds.) *A critical mind*. Berlin: Springer, pp. 369–406.

Schneider, I. (2024) 'Data stewardship by data trusts: a promising model for the governance of the data economy?' in Padovani, C. et al. (eds.) *Global communication governance at the crossroads*. Cham: Springer Nature Switzerland, pp. 333–349.

Schreiber, K., Pommerening, P. and Schoel, P. (2023) *Das neue Recht der Daten-Governance*. Baden-Baden: Nomos.

Simon, N., Markopoulos, I., Gindl, S. et al (2020) *Definition and analysis of the EU and worldwide data market trends and industrial needs for growth*. Trusts [Online]. Available at: https://www.trusts-data.eu/wp-content/uploads/2021/07/D2.1-Definition-and-analysis-of-the-EU-and-worldwide-data-market-trends-....pdf (Accessed: 27 January 2025).

Specht-Riemenschneider, L. (2023) 'Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO', *Zeitschrift für europäisches Privatrecht*, pp. 638–672.

Specht-Riemenschneider, L. and Hennemann, M. (2023) *Data Governance Act.* Baden-Baden: Nomos.

Specht-Riemenschneider, L. and Kerber, W. (2022) *Designing data trustees – a purpose-based approach*. Konrad Adenauer Stiftung [Online]. Available at: https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees+-+A+Purpose-Based+Approach.pdf/ffadcb36-1377-4511-6e3c-0e32fc727a4d (Accessed: 27 January 2025).

Spindler, G. (2021) 'Schritte zur europaweiten Datenwirtschaft – der Vorschlag einer Verordnung zur europäischen Data Governance', *Computer und Recht*, pp. 98–108.

Sprigman, C. and Tontrup, S (2024) 'Privacy decision-making and the effects of privacy choice architecture: experiments toward the design of behaviorally-aware privacy regulation', *Journal of Empirical Legal Studies*, 21(2), pp. 1–55.

Steinrötter, B. (2021) 'Datenaltruismus', *Zeitschrift für Datenschutz*, pp. 61–62.

Von Hagen, P. and Völzmann, L. (2022) 'Datenaltruismus aus datenschutzrechtlicher Perspektive', *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung*, pp. 176–181.

Waldman, A. (2018) *Privacy as trust – information privacy for an information age.* Cambridge: Cambridge University Press.

Wernick, A., Olk, C. and von Grafenstein, M (2020) 'Defining data intermediaries – a clearer view through the lens of intellectual property governance', *Technology and Regulation,* pp. 65–77.

Zingales, N. (2022) 'Data collaboratives, competition law and the governance of EU data spaces' in Kokkoris, I. and Lemus, C. (eds.) *Research handbook on the law and economics of competition enforcement*. Cheltenham/Northampton: Edward Elgar, pp. 8–49.