# Stretching the Limit, The Functioning of the GDPR's Notion of Consent in the context of Data Intermediary Services

*Yannick Alexander Vogel**

*The European Union strives to keep its Data Economy competitive and fit for the future. The proclamation of data as 'new oil' requires the envisioning of new ways to make this 'oil' available to data-driven industries. The recently adopted Data Governance Act (DGA) is a tool that increases the possibility of data-flows towards data driven industries, while simultaneously promising to maintain uncompromised data protection standards for individuals. The DGA sets the legislative framework for Data Sharing Services or Data Intermediaries. These services stand in between data subjects and data users, and serve as actor that make demand- and supply sides of data meet. When handling personal data, the Data Governance Act pivots on several notions from the GDPR, for instance that of consent. In doing so, it becomes questionable whether or not the notion of consent functions, in the DGA, in the manner as it was envisioned to function in the GDPR. A strict reading of the notion of consent makes its application in the structure of the Data Governance Act difficult to image for reasons explored in this paper. Most pressing are the elements that make up the notion of consent. Those elements being that consent should be specific, freely given and informed. These three elements are put under strain in the DGA's multi-party, data-pool, or data exchange relationships. This paper highlights how the Data Governance Act states its measures are designed to 'fully' respect the GDPR as starting point. However, when examining the notion of consent, true GDPR compliance may be an unobtainable goal or at least an unscalable one in some contexts of the Data Intermediary Services.*

*Keywords: Consent | Data Governance Act | Data Intermediaries | Data Pooling | Data Holders | Data Users | European Strategy for Data*

## I. Introduction: A European Data Economy Fit for the Future

The European Union has a particular tough nut to crack. On the one hand, there is a pressing need for more available personal data in the data economy, to foster innovation and to keep the European Union's data economy competitive.[1] On the other hand, making more personal data available to industries exists in tension with the persistent focus on individual data protection and privacy interests, which, in effect, often restrict flows of data.[2] Increasing data flows to

DOI: 10.21552/edpl/2022/2/10

* PhD Student, University of Bologna. For Correspondence: <yannickalexander.vogel@unito.it>. The author wishes to thank those who provided valuable feedback on drafts of this work and those who participated in the discussion during the Young Scholars Award during the CPDP 2022 Conference. Special gratitude goes out to Prof. M. Durante, Prof. W. Wendehorst and Prof. N. Forgó. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No 814177.

1 European Commission, 'A European Strategy for Data' COM 66 (2020), 3; European Commission, 'Impact Assessment on Enhancing the Use of Data in Europe' SMART 24 (2019), 25; I. Graef, 'Data as Essential Facility, Competition and Innovation on Online Platforms' (2016) see chapter 7.2 for an overview of how data benefits industry or leads to competitive advantage.

2 Article 1 GDPR sets the dual goal of both protecting fundamental rights and creating a market where data circulates; See, Massimo Durante, *Computational power, The Impact of ICT on Law, Society and Knowledge* (Routledge, 2021) 130.

industry, while maintaining uncompromised levels of individual GDPR safeguards, remains a difficult balancing act.[3] However, it is not the aim of this paper to argue that looser data protection safeguards will lead to better economic possibilities through increased innovation.[4] Instead, this paper analyses how the current DGA strategy, of increasing data flows in the data economy, risks diluting the original GDPR notion of consent through its application in the DGA.

In the years after the implementation of the GDPR, the European Commission understood that there is data-value left untapped. Not all data is being put to efficient use, rather, data is often locked in the hands of non-cooperating players. Many smaller sized data-users would benefit greatly from the possibility to exchange data amongst each other, therewith boosting their competitive positions. Through introducing specific legal tools in the Data Governance Act, more data can be used by more industries, and result in the creation of more value. This market-based thinking in relation to data is repeated throughout the European Strategy for Data and the Data Governance Act. Moreover, this market-based approach to data is also highlighted by the press release of 30th of November 2022 by the European Commission. When announcing the reaching of political agreement on the DGA, the press release quotes both the Commissioner for Internal Market and the Executive Vice-President for A Europe Fit for the Digital Age. Their predominantly market-based comments on the DGA are only met with a short sentence in the press release, stating that the DGA will be in accordance with EU rules, 'such as personal data protection (GDPR)'. The question remains, can Data Intermediary Services (Dis) really increase data flows to industry, without reducing any of the standards set by the GDPR, specifically regarding the notion of consent?

Ideally, both protection of the right to Data Protection of individuals and the flow of personal data for economic purposes are not seen as dichotomy but as two sides of the same coin. The DGA seeks to realize one side of that coin, increasing data flows to industry, using novel legal tools and structures. Increasing flows of data trough novel actors, such as data intermediaries or data users, will inevitably lead to data protection concerns. Especially because novel contexts are created in which the notions of the GDPR must fulfil their original function. In many cases, one simply cannot have their cake and eat it too. This paper argues that the novel mechanisms introduced in the Data Governance Act will put emphasis on data flows towards industry, at the cost of individual data protection rights, through weakening their options to express meaningful consent. As this analysis argues, the notion of consent is put under strain in the Data Governance Act, especially in the context of Data Intermediary Services. Using the notion of consent in order to increase data flows to industry risks primacy of the interests of data users over a solid consent mechanism for data subjects, for reasons explored in this paper.

### 1. Paper Roadmap

This paper argues that the notion of consent cannot function in Data Intermediary (DI) relationships where the processors and processing operations remain, in part, undetermined at the time of the retrieval of consent. On the other hand, the idea of increasing data flows, while adhering strictly to all elements of GDPR consent, will prove so laborious that it might not increase flows of data to industries in a meaningful manner at all. The following sections deal with these arguments in more detail: Section 2 sets out the Data Governance Act and defines Data Intermediaries. Section 3 elaborates on the elements of the notion of consent as specified in the GDPR. Section 4 applies the notion of consent in a specific context of Data Intermediary services. Section 5 concludes and provides further research outlook

## II. The Data Governance Act and its three regulatory Novelties

The European Strategy for Data envisions multiple avenues to make more data available to the industry, in order to create more data-enabled products and services.[5] The strategy acknowledges that enabling

3 Inge Graef, Raphael Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation' (2018) TILEC Discussion Paper No. 2018-029.

4 Julie Cohen, 'What Privacy Is For' (2013) Harvard Law Review, 126, 1919. She states that privacy is a condition for innovation and should not be juxtaposed against innovation as a hindering factor.

5 European Strategy for Data (n 1) 1.

flows of data is essential in order to boost growth and innovation.[6] The European Strategy for Data therefore proposes different novel regulations, of which the Data Governance Act is one. The Data Governance Act is only one of many different 'acts' that seeks to shape the EU's digital future, seeking to meet many regulatory goals. Some regulations seek to organise the supply and demand of data, such as the Data Governance Act and the forthcoming Data Act and other seek to correct market imbalances, such as the Digital Markets Act (DMA). However, the DGA is not the first tool aimed at increasing flows of data held by both public bodies, the private sector and individuals. Other legal instruments that increase data flows to industry are already established in the Open Data Directive and the Free Flow of Data Regulation.[7]

Therefore, the DGA is aimed at facilitating the 'opening up' of even more personal and non-personal data in specific contexts, which are not covered in existing regulations and directives. The Data Governance Act can be interpreted as having the regulatory aim to increase commercial and non-commercial use of personal data in the European Data Economy. This follows from the DGA recitals and the fact that non-personal data flows are already furthered by the aforementioned legal mechanisms.[8] The DGA in itself provides three novel mechanisms to increase data availability, for instance trough introducing a data re-use scheme under Section II. Introducing Data Intermediaries under section III and introducing a Data Altruism scheme under Section IV. The re-use scheme of section II and the Data Altruism scheme of section IV will face their own issues when it comes to GDPR consent, but those issues must be dealt with elsewhere. This paper focusses directly and exclusively on the Data Intermediary Services from section III and their relation to the notion of consent.

At the time of drafting of this paper in mid May 2022, political agreement has been reached on the DGA between the European Parliament, the Commission and the Council of the European Union. The DGA is also approved by both the European Parliament and the Council and was therefore adopted on the 16th of May 2022. However, the full and adopted text, with its final amendments, is not yet published in the Official Journal of the EU. At the time of publishing of the June 2022 edition of EDPL, this amended and final DGA text is most likely available in the Official Journal of the European Union.

## 1. Defining Data Intermediaries

This section deals with defining Data Intermediaries and does so in three manners. First it examines the text of the DGA, specifically recital 27 and 28, which clarify many points regarding Data Intermediaries. Second, it examines other sources that provide general definitions of Data Intermediaries, which are not exclusively related to EU law. Finally, instead of defining Data Intermediaries as entities or services, the analysis turns to the kinds of relationships, between different actors, that Data Intermediaries facilitate and co-create.

### a. Data Intermediaries as Defined in the Data Governance Act

Recital 27 and 28 of the GDA provide insight into what the European legislator understands when referring to Data Intermediaries. Interestingly, in the final adopted version of the DGA, the notions 'Intermediary' and 'Intermediaries' are almost completely eradicated from the DGA text. Earlier versions of the DGA mentioned Data Intermediaries as an entity in many instances. Interestingly, the final adopted version of the DGA speaks only of 'Data Intermediary Services', rather than of the entities that perform such services.[9] Of course, this begs the question if those who provide data intermediary services are also immediately data intermediaries. Article 2 (10), defining the notion of data sharing, seems to hint in that direction. It defines the notion of 'data sharing', stating that it may be done through an 'intermediary'. This is the only time the term 'intermediary' can be found in the final and adopted version of the DGA. Instead, the notion of a 'data intermediary service' is defined in more detail, in article 2 (11) of the DGA.

6 European Strategy for Data (n 1) 4, The aim is to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, (...) boosting growth and creating value.

7 Regulation 2018/1807 On a framework for the free flow of non-personal data in the European Union & Directive 2019/1024 on open data and the re-use of public sector information

8 Provisional title of the adopted Data Governance Act: European Commission, Regulation (EU) 2022/... of the European Parliament and of the Council of ...on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), 2020/0340 (COD) (2022). Hereafter: Data Governance Act.

9 Data Governance Act (n 8) Recital 27 & 28 & Article 2(11).

– 'data intermediation service' means a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, excluding at least the following.[10]

Data Intermediaries (DIs) are thus providers of 'data intermediary services' and act as a party that facilitates the aggregation and exchange of substantial amounts of relevant data.[11] However, their exact service can only be understood through understanding the notion of 'data sharing'. Being a rather colloquial term, the DGA proposes a more precise definition in article 2 (10)

- 'data sharing' means the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge

Therefore, DIs (Data Intermediaries) provide a service that connects different types of actors in the data economy and contribute to the pooling of data, as well as facilitating the bilateral or multilateral sharing of data.[12] DIs are independent from both data holders, data subjects and data users and can operate free from interference from players with large market powers.[13] Interestingly, the final amendments made before the adoption of the DGA included the word 'commercial' to refer to the service that DIs provide. Data sharing through an intermediary is now a commercial relationship between data holders, data subjects and data users. The exact nature of the commerciality in this data sharing relationship remains unclear from the wording of the DGA. Finally, the terms 'data holders' and 'data users', between which DIs mitigate, are novelties in data protection terminology. Both terms are defined in article 2 of the DGA:

– 'data holder' means a legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data.[14]

– 'data user' means a natural or legal person who has lawful access to certain personal or non-personal data and has the right, including under Regulation (EU) 2016/679 in the case of personal data, to use that data for commercial or non-commercial purposes.[15]

The third actor, the data subject, remains the same as defined in the GDPR. In essence, Data Intermediaries seek to connect two groups of parties, data holders and data subjects on the one hand and data users on the other. Those who hold data under their control, through being a legal person that holds data, or through being a data subject, are connected with those who seek to use that data for commercial and non-commercial purposes. DIs can make these parties engage in bilateral relationships, where party A (holder/subject) provides direct access to data to party B (user).[16] Alternatively, DIs can assist in the facilitation of a data pool, in which larger amounts of data are aggregated from multiple data holders, e.g. $A^1$, $A^2$. $A^3$ in to a larger pool or multilateral sharing scheme.[17] Since data subjects can also engage in data sharing, data pools or multiparty sharing schemes may simply exist out of the data of a plurality of ordinary data subjects in aggregate. DIs only provide 'services aiming at intermediating between an undetermined number of data holders and data users, excluding data sharing services that are meant to be used by a closed group of data holders and users.'[18] This conveys the idea that facilitation of data exchanges cannot be restricted to a predetermined group of data users, rather, data must flow to all data users who seek to tap into the potential of unused data.

10 Data Governance Act (n 8) Article 2(11).

11 Data Governance Act (n 8) Recital 27 & 28 & Article 2(11).

12 Data Governance Act (n 8) Recital 27 and 28 & Article 10(a).

13 Data Governance Act (n 8) Recital 27,'independent from any player with a significant degree of market power.'

14 Data Governance Act (n 8) Article 2(8) Interestingly, all earlier proposals of a data holder *included* data subjects. Only the final adopted version *excludes* data subjects as data holders of their own data.

15 Data Governance Act (n 8) Article 2(9).

16 Data Governance Act (n 8) Recital 27 and 28: '…the facilitation of bilateral data sharing'.

17 Data Governance Act (n 8) Recital 27 and 28: 'DIs that…offer services that connect the different actors have the potential to contribute to the efficient pooling of data'.

18 Data Governance Act (n 8) Recital 28: 'exclude services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group'.

To sum up, Data Intermediaries, or providers of data intermediary services, are envisioned to be the neutral buffers between data holders and data users.[19] They provide a service which is aimed at facilitating increased data sharing from data holders and data subjects to data users. This sharing can be done through bilateral or multilateral arrangements and even through contributing to pooling of data.[20] Data intermediaries are those who are tasked with making the demand and supply side of data meet, in an orchestrated and organized manner that increases trust on both sides. DIs are expected to play a key role in the data driven economy and are envisioned to be vital in the creation of future European Data Spaces.[21]

### b. Alternative Definitions of Data Intermediaries

Next to the DGA, there other definitions of DIs, definitions that are not exclusively aimed at the European regulatory framework. See for instance the definitions of Data Intermediaries in different opinion papers by the following stakeholders:

'Data intermediaries can take many forms; but what they share is a primary purpose of facilitating and managing data relations between data rights holders (such as people or businesses), depending on the parties' relationships, intentions and resources.'[22] – World Economic Forum

'Intermediaries can provide technical infrastructure and expertise to support interoperability between datasets, or act as a mediator negotiating sharing arrangements between parties looking to share, access, or pool data.'[23] – UK Centre for Data Ethics and Innovation

Although these stakeholder definitions are constructed differently compared to the text of the DGA, the gist of the notions is comparable. DIs envisioned function remains largely the same for the stakeholder definitions and the DGA definition of providers of data intermediary services. That is, mediating between those who have data and those who seek to use data. The difference is that the DGA does not refer to DIs as entities, but instead only to the service which they provide, while the stakeholder definitions refer to DIs as entities. The exact organisational form in which a DI provides its service is not set in stone in either the DGA or the stakeholder definitions. Instead, multiple different organisational forms are possible. Think of data trusts, data exchanges, Personal Information Management Systems (PIMS), data cooperatives, data custodians and many others.[24] The different organizational architectures in which DIs can operate remain varied and therefore hinder the possibility of clearly defining Data Intermediaries as a specific entity or actor.

### c. Defining Data Intermediary Services Through Created Relationships

The two previous sections highlight how it is difficult to define DIs with great accuracy, since the definitions remain rather broad and leave open many possibilities. One may deduct from the text of the DGA that a DI is a neutral entity, which mitigates between data users and data holders and provides data from one party to the other. Moreover, if the DGA in general is aimed at opening up more personal data to industry, DIs must in some way also facilitate that aim. Given this unclarity, and with taking notice of the varying stakeholder definitions of DIs, it is more important to examine how DIs function, rather than to pinpoint what they are exactly. What is interesting in that regard is that there are four types of relationships, or exchanges of data between actors, that start to exist from the data sharing services provided by DIs. The depiction of the created relationships that DIs can facilitate is as follows:

1) Data holders provide personal data under their control, directly to individual data users (bilateral relation)
2) Individual data subjects provide their own personal data, directly to individual data users (bilateral relation)
3) Data holders provide personal data under their control to DIs, which aggregate, or pool, the data and provide multilateral or pool-access to an undetermined number of data users (multilateral relation)

---

19 Data Governance Act (n 8) Recital 33: 'neutrality of data intermediation services providers with regard to the data exchanged between data holders or data subjects and data users'.

20 See (n 16) and (n 17).

21 Data Governance Act (n 8) Recital 27: 'are expected to play a key role in the data economy'.

22 World Economic Forum, 'Advancing Digital Agencies, The Power of Data Intermediaries, Insight Report' (2022) 9.

23 Centre for Data Ethics and Innovation, 'Unlocking the value of data: Exploring the role of Data Intermediaries' (2021) 8.

24 Centre for Data Ethics and Innovation (n 23) 9; Data Governance Act (n 8) Recital 27: 'or the creation of platforms or databases enabling the sharing…'

4) Individual data subjects provide their own personal data to DIs, which aggregate, or pool, the data and provide multilateral or pool-access to an undetermined number of data users (multilateral relation)

In relationships one and two, DIs merely facilitate the technical and legal structure between parties on either side of the demand and supply side of data. In the simplest scenario, DIs merely introduce the two parties to each other and facilitate the legal and technical details of the access to or transfer of data between them. The relationships under headers one and two are bilateral, between data holders/subjects and data users, therefore these relationships are easier to understand when compared to multi-party agreements or pool-relationships. In relationships three and four, the situations are different, in such multilateral structures, the DIs actively provide a technical infrastructure between an 'undetermined' number of actors on the data-user side of the data pool. Such relations are inherently more complex due to the increase of parties and the creation of more relationships. Recital 27 and 28 of the DGA specifically voice the idea of multi-party relationships, with an 'undetermined' number of participants, in Data Intermediary Services in recitals 27 and 28.[25]

The use of the word 'undetermined' confirms that the DGA seeks to create relationships between a large group of actors, therefore removing barriers for data access for SME's and start-ups. The DGA specifically excludes sharing services that depend on a closed group of data holders, in which all actors are determined rather than undetermined.[26] The previous has implications for the manner in which the notion of consent functions, but the issues are not evenly distributed amongst all of the four created data exchange relationships. Especially problematic are scenario three and four, which deal with an undefined, or in the words of the DGA, 'undetermined', number of data users. To see where the problems present themselves it is required to examine the notion of consent in more detail.

## III. The Elements of Consent Under the General Data Protection Regulation

Processing of personal data, governed by the GDPR, can only take place when there is a legal basis for that processing. In other words, the processing must be lawful. The GDPR both requires and provides these legal grounds.[27] One of those grounds, and arguably the most widely used, is based on the consent of a data subject to processing activities, captured in articles 6(1)a, 7 and 8 of the GDPR. Consent to data processing under the GDPR requires a clear affirmative act that is informed, specific, unambiguous and freely given.[28] When consent is not informed, freely given, unambiguous and specific, it is not valid consent, since the four elements are cumulative. These elements require some more elaboration:

### 1. Unambiguous Indication of Wishes

For consent to be valid it must constitute an active movement by a data subject. Consent cannot be implied from the context of the relationship between a data controller and a data subject. As confirmed by the ECJ in the Planet 49 case, pre-ticked consent boxes or silence do not constitute valid consent.[29] Since pre-ticked boxes and silence are no active movements by data subjects they are therefore no unambiguous expression of wishes.

### 2. Freely-Given

Consent cannot be retrieved from persons in the case of a clearly crooked power imbalance between the requester for consent and the data subject. Think for

25 Data Governance Act (n 8) Recital 27 and 28: 'This Regulation should cover services which aim to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other' and '… that offer services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing'.

26 Data Governance Act (n 8) Recital 28.

27 Elena Gil González and Paul de Hert, 'Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles' (2019) 19 ERA Forum 4, 599.

28 See generally: Eleni Kosta, Consent in European Data Protection Law (Nijhoff Studies in European Union Law, 2013); Bart Schermer et al, 'The Crisis of Consent, How Stronger Legal Protection may lead to Weaker Consent in Data Protection' Ethics & Information Technologies (2013) 7; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (2020) 14/15

29 CJEU C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH

instance of an employee/employer relationship or a public entity requiring consent from its citizens.[30] Put best by the EDPS: 'The element 'free' implies real choice and control for data subjects.'[31] Therefore, consent may also not be bundled with non-negotiable parts of the terms and conditions to which users must agree. Such bundling renders consent to be given in a manner that is not free. Naturally, many different circumstances and contexts could be envisioned that hinder this 'freely given' element.

## 3. Informed

Data subjects must be informed as to the data processing activities and actors which they are asked to consent to. M. Botta argues that consent is often not informed at all: 'users 'agree' with policies at large but are not aware of what exactly they consent to'.[32] Theoretically this statement is tricky, if users are unaware of what they consent to, arguably they have not consented at all. Data subjects in such cases merely 'agreed' to data processing, which is not a correct legal basis for processing of personal data.[33] However, in its guidance on the meaning of consent, the EDPB stresses that the data subject must be in a position where he or she can be informed.[34] The EDPS thus sets out guidance for the manner in which data subjects should receive information, rather than demanding that data subjects actually digest the information that is presented to them by the consent seeking data controller. L. Moerel, argues that data subjects often remain uninformed regarding the processes they consent to, nor do they have a real possibility to pick apart the information they are served in cryptic cookie banners and privacy policies.[35] In order for data subjects to be informed, they need to have access to at least the identity of the data controller, the purpose of the data processing, the type of collected data and the existence of the right to withdraw consent.[36] Data controllers that wish to rely on the notion of consent for their processing activities must be named at the time that consent is retrieved. Other controllers may not be given access to the data of data subject when they are not mentioned in the original consent request. With regards to the identity of data processors, not all have to be named in the consent request. However, their identity must be specifically named by the controller at the time of the collection of data, under article 13 and 14 of the GDPR.[37]

## 4. Specific

The specificity of consent to processing is another crucial element of GDPR consent. According to the EDPS, specificity is closely related to granularity of consent and the element of being informed. In the words of the EDPS, specificity: 'aims to ensure a degree of user control and transparency for the data subject'. The specificity-element of consent safeguards three matters. First it acts as a safeguard against function creep.[38] Second, it furthers the granularity of consent requests and finally, it separates information relating to obtaining consent from information on other matters.

The specificity-element therefore primarily protects data subjects from the widening, or creeping, of the data processing activities which they consented to. The EDPS refers to the notion of purpose limitation in this regard, stating that 'specific consent' (...) 'functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.'[39]

One key function of specific consent is therefore that it protects against function creep through ensuring that third parties cannot process personal data in a manner that is unanticipated by the data subject. Specific consent ensures that data subjects know who is doing the processing and what the processing en-

30 European Data Protection Board Guidelines on Consent (n 28) 7.

31 Ibid.

32 Marco Botta and Klaus Wiedemann, 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (2019) Antitrust Bulletin 64, 3, 433.

33 Marco Botta (n 29) 432.

34 European Data Protection Board Guidelines on Consent (n 28) 15/16.

35 Lokke Moerel, 'Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof' (2018) Tilburg University, 24, 49, 51.

36 European Data Protection Board Guidelines on Consent (n 28) 15.

37 Ibid.

38 Further reading on the notion of function creep: Bert-Jaap Koops, 'The Concept of Function Creep' (2021) Law, Innovation and Technology, 29-56.

39 European Data Protection Board Guidelines on Consent (n 28) 14.

tails. Their consent is specific to both the identity of the data processing actors and the processing activities of those specific actors.

### 5. Court of Justice of the European Union Case law on Consent

One could argue that the working definition of consent, in practice, is just more relaxed than the consent definition that follows from a strict reading of the GDPR. If one truly complies with all the standards set in the GDPR for valid consent, then obtaining valid consent is a tedious exercise. In practice, persons may perceive consent requests as just an annoyance between them and the content they seek to access, rather than a carefully regulated process.

However, this relaxed reading of the notion of consent is not accepted by the European Court of Justice. Instead, the European Court of Justice has, in its recent case law, cracked down on the notion of consent. For instance, in case Planet 49, the court states that pre-ticked consent boxes do not constitute valid consent.[40] In case Orange Romania, the court explains the need for individuals to be able to understand the consequences of their consent.[41] Specifically, the court states in paragraph 52: ' it is for the data controller to demonstrate that the data subject has, by active behaviour, given his or her consent to the processing of his or her personal data and that he or she has obtained, beforehand, information relating to all the circumstances surrounding that processing, in an intelligible and easily accessible form, using clear and plain language, allowing that person easily to understand the consequences of that consent, so that it is given with full knowledge of the facts.'

From this flows that the approach of the ECJ towards consent is neither relaxed nor slacking. Rather, the ECJ reiterates the strict demands for consent to be valid and perhaps even sharpens them a tad. Of course, this puts a great burden on consent-requesters since it mandates them to make sure that data subjects have the information required to arrive at the 'full knowledge of the facts'.

## IV. Stretching Consent in Data Intermediary Mediation Contexts

This section deals with three issues. First is argues that consent is the preferred legal basis for Data Intermediaries processing activities over other possible legal bases provided by the GDPR for the processing of personal data. Second it argues that, in bilateral DI relationships, the problems regarding DI services and consent are minor. Finally, it argues that in multilateral data relationships, facilitated by data intermediaries, use of consent as legal basis for processing will seriously stretch the limits of GDPR consent through complicating several elements of consent.

### 1. Consent as Legal Basis in Data Intermediary Contexts

The first issue to deal with is the choice of the legal basis of processing in itself. Consent is only one of the six legal bases for the processing of personal data. Relying on consent is therefore not the only available legal basis for processing which DIs can opt for. The DGA however, seems to be hinting at the use of consent as legal basis for processing in article 2(10), where it stresses the voluntary character of sharing data through DIs. If data sharing services in the DGA are defined as being 'based on voluntary agreements', it would be difficult to argue that consent would not play a key role.[42] Moreover, recital 30 of the DGA states that certain DIs, when handling personal data, would assist individuals in exercising GDPR rights, in particular, managing their consent to data processing.[43] Other clues can be found at the receiving end of the consent request. Both Dawex and Meeco, two DIs based in the European Union, repeat the idea of consent of data subjects in order to manage their data transfers. Meeco does so through what they call their 'Consent Engine', stating that it 'enables people to decide who can use their data, for how long and for what reason'.[44] A similar notion is proposed by Dawex, although worded a tad more cryptic. Dawex

40 CJEU C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH

41 CJEU C-61/19 Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

42 Data Governance Act (n 8) Article 2(10).

43 Data Governance Act (n 8) Recital 30.

44 See, <https://www.meeco.me/meeco-whitepaper> accessed 17 March 2022; See, <https://www.Dawex.com> accessed 17 March 2022.

offers 'full control over interfaces' and 'advanced rights management' to its users when it comes to deciding on the flow of their data. Therefore, both the DGA and emerging European Data Intermediaries seem to envision consent as the preferred legal basis for processing of data in DI contexts rather than relying on other legal bases for data processing.

## 2. Applying Consent in Data Intermediary Mediated Bilateral Relationships

In the case where a DI mediates between a data subject/holder and a data user, where their relationship is bilateral in nature, the issue of retrieving valid consent does not seem to be very problematic. The elements of valid consent can be met in the same manner as they are being met in current digital consent requests. The nature of the relationships in these bilateral data exchanges are as the GDPR envisioned, namely, between parties that can identify each other and understand each other's practices with reasonable effort.

## 3. Applying Consent in Data Intermediary mediated Multilateral Relationships

The situation changes when a DI mediates between an undetermined number of data users and an indefinite number of data holders/subjects. As became clear in section 3, if data subjects cannot be informed as to the specific processing operations and the specific identity of all those who use their data, consent cannot be validly retrieved from these data subjects. In other words, the GDPR does not seem to have envisioned for consent to function in a multilateral (pool) relationship with an undetermined number of data users that cannot be defined accurately at the time of retrieval of consent.[45] Naturally, if the identities of parties that seek consent to use data cannot be specified, neither can their exact processes of 'data usage'. This is problematic, since consent is always specific to its requester, the parties involved and the specific processes involved. Therefore, using consent as legal basis for data-usage, with an undetermined number of data users is problematic. When adhering to the letter of the GDPR's notion of consent, an undetermined number of users can simply not be specific.

### a. From a 'Full Knowledge Test' to an Undetermined Number of Unknowns

In the case where Data Intermediaries mediate between an undetermined number of data users and data holders/subjects. Data subjects that are asked to express their consent to processing operations can, by the nature of an 'undetermined number' of data users, hardly arrive at 'full knowledge of the facts' regarding the consequences of their consent. It will be impossible for data subjects to be informed regarding all those who access their data in a data pool or in a multiparty setting with an undetermined number of users. Nor will it be possible for data holder/subjects to be informed regarding all the 'information relating the circumstances surrounding that processing', as the ECJ requires in its case law.[46] Arriving at such a level of being informed would mean that data subjects, or data holders, understand an enormous amount of processing activities by a large and undetermined number of data users. Naturally, with more and more data users accessing and using the personal data, more and more risk of persons being unable to inform themselves fully arises. Therefore, data subjects/holders deal with a great amount of 'unknowns' which they are expected to be informed of, both in terms of the processing activities and the actors involved. Applying consent in the context of an undetermined amount of data users, as the DGA envisions, is therefore directly in confrontation with the idea of consent being both specific and informed. The recent case law of the ECJ has only strengthened this point, by tightening the reins on consent in its recent case law. Therefore, there is a real risk that the test that the GDPR, the EDPB and the ECJ set for valid consent, cannot be met through the architecture created in the DGA.

### b. Troublesome Scalability of Valid Consent

Alternatively, one could envision a situation in which consent, in DI multiparty contexts, would function

45 European Data Protection Board & European Data Protection Supervisor, 'EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' (2021) 29/30.

46 CJEU C-61/19 Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) para 40.

in compliance with the high standards of GDPR consent. In that case, consent would have to be renewed in every instance where a new type of processing is engaged in by any of the data users.[47] Consent would also have to be renewed when a new party is added to the list or pool of data users, which is already undetermined. Protection against an unnoticed increase of parties involved and processing activities, also known as function creep, is exactly why the element of specificity was created. In the case of introduction of new data users and new data processing activities, renewal of consent becomes mandatory.[48] Simply put, new data users or new processing activities require a new consent request. With an undetermined number of data users, changes in their processing activities will be rapid and continuous, therefore, so will consent renewal requests. Compliance with the elements of valid consent then seems utterly unscalable on the side of the data subjects.

### c. Between a Rock and a Hard Place

Given the previous, it would be hard to imagine that DIs can meaningfully manage consent from data holders/subjects when the number of parties increase towards a large undetermined number of actors on both sides of the data gap. Alternatively, understanding these large multiparty relationships as a plurality of individual bilateral relationships requires novel technological infrastructures. It is questionable whether these currently exist, or if the text of the DGA should require such technological fixes for problems of its own creation in the first place. The problem of using consent in to facilitate access to data for all SMEs and start-ups, in a non-discriminate manner, remains in place. It is the wording of the DGA, and its 'undetermined' number of data users that causes the problem.

The previous creates a situation where both depicted alternatives seem equally unlikely. Adherence to valid consent, with its information and specificity requirements, is not as scalable as the DGA makes it appear to be in some of the data intermediary relationships it creates. At the same time, these exact multi-party relationships, of increased data supply and data demand, are the reason the DGA was created in the first place. This results in a classic situation where one cannot satisfy both options at the same time. Either the promise of massive amounts of data provided to industries is not delivered on, or the notion of consent is stretched beyond reasonability.

### d. Reversal of the Consent Initiative and Interests of Data Subjects

As further point of concern, the original narrative of consent requests also seems reversed in the DGA. In classic situations, persons are almost exclusively confronted with consent requests out of their own initiative. Meaning, when one accesses a website, or wishes to use a digital service, a consent request is anticipated. Rarely is one confronted with a consent request which is not initiated from the side of a data subject. Consent requests do not come out of the blue, but rather follow from the choice of data subjects to interact with data controllers. The created DI relationships depict a different scenario. When an indefinite number of data users approach an aggregation of data retrieved from data subjects/holders, the initiative for the establishment of a consent relation comes from the side of the data users.[49] It is the data user that seeks access first, and therefore takes the initiative to establish a data sharing relationship. This reverses the primacy on initiative by the data subjects, and places initiative at the data users.

This ulterior issue will have to be grasped with as the DGA comes into force, but it is another reason why the notion of consent, applied in the DGA, may lead to unforeseen issues. If data subjects are fatigued with consent request of processing operations that they themselves instigate, this fatigue will only grow when data subjects are presented consent requests following from relationships that they themselves did not instigate. Even more interesting, DIs will make sure that individuals do not share more data, to data users, than 'is in their own interest'.[50] It leaves to be seen how sharing data with undetermined parties is in the interest of data subjects in the first place. In that sense, the DGA is designed to help individuals make more data available than is normally in their interest, but provides a safe environment to so. One could argue, as the EDPS and EBPD have done in different contexts, that using specific GDPR notions in

47 European Data Protection Board Guidelines on Consent (n 28) 14.

48 Ibid.

49 Data Governance Act (n 8) Recital 30.

50 Ibid.

novel contexts might result in inconsistency with the spirit and the letter of the GDPR.[51] This problem of reversal of initiative and the countervailing interests of subjects and users seems to be an example of such inconsistency with the spirit of the GDPR.

## V. Concluding Remarks and Future Outlook

This final section deals first with the conclusion of this paper based on the previous discussion and second, with a future research outlook with a broader perspective.

### 1. The Limits of the Notion of GDPR Consent

First, regarding the stretching of the notion of consent. The notion of consent is put under strain through its application in contexts for which it was not originally designed. The application of GDPR consent, in most multi-party DI facilitated agreements, faces an interesting trade-off. Applying consent, as it was designed to be applied in the GDPR, will take much of the wind out of the sails of the aims of Data Intermediary Services. It would be hard to image how consent can facilitate the 'aggregation and exchange of substantial amounts of relevant data', as the DGA seeks to effectuate.[52] It leaves to be seen how DIs can apply the strict reading of the notion of consent while at the same time deliver on the promise of making significantly more data available to industries. At the same time, if DIs succeed in making enormous amounts of personal data available to industries, then that would come with an equally enormous 'consent workload'. DIs would have to manage, facilitate an incredible amount of consent requests while also paying fiduciary duties to the data subjects and holders. It would therefore be hard to envision a scenario where both increased data availability and an intact notion of valid consent are realized, without compromising on either side.

More specifically, the stretching of the notion of consent, in specific contexts of Data Intermediary Services, becomes apparent through impossibility of adherence to two of consent's constitutive elements. Those two elements being, the requirement for consent to be specific and for consent to be informed, in the manner that the legislator and case law prescribes. The risk of failure to adhere to these two constitutive elements in DI contexts is a direct result of the architecture that the DGA seeks to promote, namely, data sharing with an undetermined number of data users. The notion of consent is therefore stretched to its limits or perhaps beyond its limits. GDPR consent is simply not created to facilitate these types multi-party of data sharing relationships. At the same time, not stretching the limits of consent likely results in not reaching the regulatory goals that the Data Governance Act sets.

### 2. The Limits of the GDPR as a Solid Foundation for Future 'Data Legislation'

The previous also opens the door to a second, more fundamental discussion. While many have proposed changing the GDPR in one way or another, the nature of the need for such change itself has transitioned.[53] With many new legislative tools on the horizon, such as the Data Act, the Artificial Intelligence Act, the Digital Services Act and the Digital Markets Act, it becomes increasingly more difficult to ensure full congruency with the GDPR. This paper has demonstrated so for the specific use of GDPR consent in a specific Data Intermediary context, but the issue is quite likely much deeper and found in many more contexts. The idea that rings throughout the European Data Strategy and the DGA, of creating legislation that is in 'full compliance' with existing data protection law, may in itself not be the wisest long-term strategy.[54] With the GDPR as a cornerstone for many emerging legal instruments, incongruency is bound to present itself. The need for adaptation of established notions is now found in its interlocking with novel legal instruments, that seek to 'fully comply' with the GDPR.

Therefore, perhaps it is more fruitful to reassess the balance of the interests of parties on both the side

51 European Data Protection Board & European Data Protection Supervisor (n 45) 13.

52 Data Governance Act (n 8) Recital 27.

53 For instance: Paul de Hert and Guillermo Lazcoz, 'Radical rewriting of Article 22 GDPR on machine decisions in the AI era' (2021) European Law Blog. They argue that article 22 GDPR is on the verge of extinction.

54 European Strategy for Data (n1) 1.

of data supply and data demand, rather than to use important established notions in a dubious manner.[55] Making meaningful amendments to existing notions is preferable over fully respecting the GDPR on paper, and turning a blind eye to the impossibilities that brings in practice. With more and more legislative tools focussing primarily on 'how to do things with data', recalibration of rules, notions and concepts rather than 'fully respecting' existing law seems to be a more viable strategy for the future.

55 In the spirit of Massimo Durante, *Computational power, The Impact of ICT on Law, Society and Knowledge* (Routledge, 2021) 130-131.