Towards a technologically assisted consent in the upcoming new EU data laws?
Chomczyk Penedo, Andrés

Published in:
Privacy in Germany

DOI:
10.37307/j.2196-9817.2022.05.05

Publication date:
2022

Document Version:
Proof

Link to publication

Citation for published version (APA):
Chomczyk Penedo, A. (2022). Towards a technologically assisted consent in the upcoming new EU data laws? Privacy in Germany, 5(22), 180-187. https://doi.org/10.37307/j.2196-9817.2022.05.05

Copyright
No part of this publication may be reproduced or transmitted in any form, without the prior written permission of the author(s) or other rights holders to whom publication rights have been transferred, unless permitted by a license attached to the publication (a Creative Commons license or other), or unless exceptions to copyright law apply.

Take down policy
If you believe that this document infringes your copyright or other rights, please contact openaccess@vub.be, with details of the nature of the infringement. We will investigate the claim and if justified, we will take the appropriate steps.
Towards a technologically assisted consent in the upcoming new EU data laws?

Andrés Chomczyk Penedo

The European Commission (Commission) put forward an ambitious proposal package of new legislation for the digital economy, including the Digital Markets Act, the Digital Services Act, or the Data Governance Act. Despite their different scopes, they all share a recurring topic: the relevance of (personal) data in enabling a data-intensive economic model around data sharing and the role of data subjects in granting permission to do so. As such, the purpose of this article is to explore how the Commission and other EU institutions intended to strengthen consent in these novel data regulations through technological tools but also novel assistance duties, but also the potential shortcoming around this approach.

I. Introduction

2022 is on its way to becoming another landmark year for EU lawmaking, just like 2016 when the General Data Protection Regulation (GDPR) was adopted. The European Commission (Commission) put forward an ambitious proposal package of new legislation for the digital economy to tackle a wide range of issues: from how data, both personal and non-personal, should be used for societal benefit,1 up to balancing the asymmetries found in the platform business model.2 This complex myriad of proposed regulations deals with how (personal) data is generated, used, and shared through large online platforms.3

Part of the legislative agenda has already been adopted or is undergoing its last formal steps, including key regulations such as the Digital Markets Act (DMA),4 the Digital Services Act (DSA),5 and the Data Governance Act (DGA).6 However, some of the other regulatory instruments envisaged are still in the works, such as the Data Act (DA)7 and the European Health Data Space (EHDS),8 or in the legislative pipeline, as for the rest of the data spaces.9

Each piece of this complex regulatory framework deals with specific scenarios, such as ensuring competitive market conditions through the DMA or how to effectively moderate online content with the DSA, just to name a few examples. However, as noted years ago by the European Data Protection Supervisor (EDPS),10 they take a mixed approach by combining competition, data protection, and consumer protection law to effectively tackle the challenges of the digital economy. In this respect, they all share a recurring topic: the relevance of (personal) data in enabling a

1 Andrés Chomczyk Penedo is a PhD researcher at the Vrije Universiteit Brussel. He conducts research on the development of a duty of assistance under the GDPR as a MSCA fellow in the PROTECT ITN (Grant Agreement No. 813497).
4 For the purpose of this article, it shall be used the final text approved by the European Parliament: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0270_EN.html.
5 For the purpose of this article, it shall be used the final text approved by the European Parliament: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html.
7 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) COM(2022)68 final.
9 ‘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’ (n 1) 22–23.
data-intensive economic model around data sharing and the role of data subjects in granting permission to do so.

These rules have not amended the GDPR but rather intend to build upon it, acknowledging its achievements when it comes to securing the right to personal data protection. However, the multiplicity of legislation and how these legal instruments interact with each other might produce tension with the GDPR and between each other. Previous attempts relying on this formula proved challenging, despite its apparent simplicity. The tension between the GDPR and other field-specific legislation dealing with personal data has shown in the past the need for interpretative integration to mitigate short-circuits between rules, as was the case with the Payment Services Directive 2.

As it will be explored in this contribution, consent has been given a key role within this new regulatory landscape. As a legal basis for processing personal data, consent presents numerous requirements to be considered as validly collected. In this sense, the first impression of this legislative package could make one wonder if the Commission omitted the issues that consent has been facing as a legal basis for quite some time. As such, the purpose of this article is to explore how the Commission and other EU institutions intended to strengthen consent in these novel data regulations.

Therefore, this article is structured as follows: Section II will present the existing efforts to govern personal data flows within platforms and the shortcomings of previous attempts to regulate this; Section III shall introduce the new regulatory developments and how they relate to the GDPR; in Section IV will address the approach to consent in these novel data-related regulations and how it is expected to assist data subjects; and, finally, Section V will provide some preliminary conclusions regarding this complex puzzle put in place around consent.

11 Recital 12 DMA, Recital 10, and Art. 1a. 4. (g) DSA, Art. 1.3. DGA, and Art. 1.3. DA.
12 In this respect, both the EDPS and the EDPB have provided their opinion in different documents regarding this to further improve the link between the GDPR and these new data regulations (see ‘Joint Opinion 02/2022 on the Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)’ (European Data Protection Board – European Data Protection Supervisor) Joint Opinion 02/2022; ‘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)’ (European Data Protection Board – European Data Protection Supervisor 2021) Joint Opinion 03/2021; ‘Opinion 02/2021 on the Proposal for a Digital Markets Act’ (European Data Protection Supervisor 2021) Opinion 02/2021; ‘Opinion 01/2021 on the Proposal for a Digital Services Act’ (European Data Protection Supervisor 2021) Opinion 01/2021.
18 Art.9 Platform-to-Business Regulation.
19 Art.5.5. [a] Platform-to-Business Regulation.
20 Christoph Busch, ‘Regulation of Digital Platforms as Infrastructures for Services of General Interest’ (Friedrich Ebert Foundation 2021) 9/2021.
22 Art.94.2 Payment Services Directive 2.
previously mentioned provision is included in the ‘data protection’ portion of the directive, it is questioned to what exactly was it referring to an explicit consent as understood in the GDPR, or to a special kind of consent given to perform certain actions, i.e., the performance of a contract, which involves personal data.

Given this, it was necessary for the intervention of the European Data Protection Board (EDPB) to bridge the gap and interpret the personal data protection-related provisions. In this respect, the EDPB adopted the criteria that Art. 94.2 is referring to as the explicit consent the payment services users have to provide when using certain services, therefore making the legal basis the execution of a contract. The answer to this wasn’t convincing as elaborated by the legal literature. Nevertheless, it provides some remarks to be taken into consideration for this analysis as, if there is an underlying service being provided, then the legal basis for any data processing associated with it would be, in principle, the performance of a contract, even if the legal framework would suggest consent as it.

III. The new legislative package: an overview of the upcoming regulatory landscape

The purpose of this section is to briefly summarize the new data-related regulations and reflect on how personal data processing is addressed in each of them. By doing so, it would be possible to draft how these interact with each other and with regards to the GDPR, particularly around the legal basis to enable large processing of personal data.

1. The Digital Markets Act

The DMA seeks to provide, according to its Art. 1.1, ‘(…) harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users’ to foster better competition conditions for businesses and users relying on platforms. This is done through the adoption of ex-ante rules that apply to certain digital services, known as core platform services, but only when provided by a gatekeeper. Besides this, it sets an improved antitrust regulatory framework, with strong powers for the Commission in its quest against abusive platforms operators.

These gatekeepers are obliged to comply with the DMA’s obligations but also to refrain from acting in certain manners; these have been considered conducts that can foster or diminish competition, respectively. Among these, it is possible to include the following: abstain from using users’ personal data to provide online advertising services, allow businesses to offer the same services provided through the platform via another venue with different economic conditions, avoid tied sales, a prohibition on the use of data generated by businesses to compete with them if not publicly available, favour its own products or services in rankings, or ensure certain minimum interoperability requirements, among many others.

The DMA has dedicated considerable attention to how personal data generated in platforms can be used by businesses, users, or even the platform itself, particularly as personal data can be a deciding factor in ‘making or breaking’ the entrance of new competitors into a particular market. In this sense, it puts in place a general prohibition for the following: using personal data to deliver an online advertisement to end users for third parties; combine personal data from different services, provided either by the gatekeeper or relying on data from third parties; use data from different services provided by the gatekeeper on a separate basis, and enroll users to combine personal data.

Particularly regarding these prohibitions, it is recognized that gatekeepers collect information from a wide array of third parties on a particular data subject. This is done, primarily, to offer a free service to users in exchange for delivering online advertisements. To balance this, the DMA intends to put data subjects at the forefront and empower them to counter this practice. They would be able to decide whether they agree to these activities and, if not, receive an ‘ad-free’ service. In this respect, the ad-free or ad-less version should be equivalent to the regular version unless processing personal data is necessary for the service.

Finally, the DMA also sets certain limits and requirements for using data given its anticompetitive consequences. In this sense, a gatekeeper can only use publicly available data generated or provided by business users, a provision very much in line with requirements already found in the P2B Regulation. This effective and free-of-charge access could be ensured by (…) appropriate technical measures, for example by putting in place high quality application programming interfaces or integrated tools for small volume business users.

24 Art.9.2. (a) GDPR.
25 Art.65.1. (b), 6.5.2. (a), 66.2, 66.3. (c), Art.67.2. (a) Payment Services Directive 2.
27 Ibid 37.
28 Art.6.1. (b) GDPR.
29 Ferretti (n 23).
30 While not discussed in this piece, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Digital Content Directive) provides a different approach. In it, the relevance of consent as a legal basis when content or services are ‘paid for’ with personal data was address in its provisions, requiring that the requirements of consent under the GDPR were fulfilled, particularly the freedom in providing such consent. In this sense, Recital 38 clearly states that the Digital Content Directive ‘[…] should not regulate the validity of the consent given’ and, therefore, it recognises the GDPR’s prominence on this. In contrast, the Payment Services Directive 2, and particularly EDPB’s guidance, affected the legal protection granted by consent for processing personal data.
32 Art.2(2) DMA.
33 Art.2(1) and 3 DMA. To be considered a gatekeeper, it is necessary to meet a three-prong quantitative and qualitative assessment under Art.3 DMA.
34 Arts. 16 through 26 and 29 through 33 DMA. On top of this, the Commission can also lean on other disclosed information under Art.14 to further exercise its powers.
35 Art. 5, 6, and 7 DMA.
36 Art. 5.2. (a) DMA.
37 Art. 5.3 DMA.
38 Art. 5.8 DMA.
39 Art. 6.2 DMA.
40 Art. 6.5 DMA.
41 Art. 7.2 DMA.
42 Recital 72 DMA.
43 Art. 5.2. (a) DMA.
44 Art. 5.2. (b) DMA.
45 Art. 5.2. (c) DMA.
46 Art. 5.2. (d) DMA.
47 Recital 36 DMA.
48 Recital 37.
49 Art. 6.2 DMA.
50 Recital 60 DMA.
2. The Digital Services Act

In contrast to the intended scope of the DSA is ‘(...) to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment, that facilitates innovation, where fundamental rights enshrined in the Charter, including the principle of consumer protection are effectively protected.

This is done, according to Art. 1.2., through setting up: (i) a legal regime for intermediary service providers’ liability, expanding upon the terms in the eCommerce Directive; (ii) ex-ante obligations to certain intermediary service providers dealing with a wide range of issues; and (iii) common implementation and enforcement rules.

The obliged subjects under the DSA are intermediary services, with different compliance requirements depending on the effective services provided by them, from simply obligations of disclosing how every intermediary service restricts their service in their terms of use, up to complex risk assessment for very large online platforms.

Regarding this latter category, to whom most of the data protection-related issues apply, it follows some of the criteria found in the DMA to classify certain intermediary service providers as such, namely the 45 million users requirement.

One of the main concerns that the DSA tackles is the regulation of the online advertising business model, which relies heavily on the use of personal data to effectively assign advertisements to the ‘right’ individual. In this sense, the DSA works in tandem with the DMA by providing further rules to govern online advertisement as well as how these ads are shown to individuals.

If personal data was used to assign an ad to a data subject, this must be explained with all the information required under both the DSA, as well as the GDPR particularly when it comes to the data rights available to such processing or if consent was needed to process the personal data that assigned the ad to somebody.

3. The Data Governance Act

The DGA has three main purposes: (i) govern how data, both personal and non-personal, held by public bodies can be re-used; (ii) set the rules for the provision of certain data intermediation services; (iii) and ground the data altruism. While the DSA has been considered by many as the DMA’s main companion to effectively tackle the challenges posed by online platforms, when it comes to how data, particularly personal data, can be processed, the DGA takes a leading role in this respect, particularly in complementing the GDPR in the governance of personal data use, sharing and reuse, for example by adopting its definition of consent.

The first portion of the DGA focuses on how data held by public bodies can be re-used for other purposes. This is aligned with the broader EU Data Strategy, which places a great deal of importance on ensuring that data can be shared between parties to enhance datasets and, in theory, achieve further economic and societal growth.

While the re-use of public-held data has been in the spotlight since the EU Open Data Directive, data intermediation services and data altruism represent novel data sharing schemes. As for the first category, it is possible to include in it any service, including those for-profit, that seek to enable data sharing between data subjects and data holders with data users, such as example data cooperatives. On the other hand, data altruism implies the ‘(...) voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them (...) for objectives of general interest (...)’.

Regarding data intermediation services, the DGA expects them to play in key role in assisting data subjects in understanding the terms under which their personal data might be processed. Recital 30 states that these ‘(...) data intermediation services providers seek to enhance the agency of data subjects, and in particular individuals’ control over data relating to them.’ For example, and connecting with the DMA, it would be possible to think about a data intermediation service that helps data subjects in assessing the differences between a service with ads and its ‘ad-free’ version to consent or not under the DMA.

Turning to data altruism, Recital 45 acknowledges the potential benefit from data subject voluntary sharing information for general interest purposes. Particularly, given that this kind of data processing might involve special categories of personal data, consent is expected to play a key role in the operation of data altruism organizations. However, given the wording used in the Recital, it is possible to wonder whether another legal basis would be available or not for data altruism organizations to conduct their businesses, particularly when the processing ‘(...) is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (...)’.

The DGA is set to become another cornerstone legislation of the EU personal data protection regulatory framework by granting a set of rules for many data-related services. By introducing specific rules for ‘trusted’ third parties that data subjects can ask for help in managing their personal data, will constitute a meaningful change from existing rules that put all the burden alone and exclusively on data subjects.

4. The Data Act

Finally, the DA constitutes the last piece of proposed legislation by the Commission dealing with how data can, and should, be used in the digital economy. The DA would establish ‘(...) harmonised rules on making data generated by the use of a product or related service available to the user of that product or service, on the making data available by data holders to data recipients, and on the making data available by data holders to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest.’


60 Art. 2(11) DGA.
61 Art. 2(5) DGA.
62 Art. 2(10) DGA.
63 Art. 12. (m) and (n) DGA.
64 Recital 30 DGA.
65 Art. 5.2. in fine DMA.
66 Recital 45 DGA.
67 Recital 50 DGA.
68 Art. 9.2. (j) GDPR.
69 Art. 1.1 DA.
Therefore, the DA's objective is far more reaching than just setting forth new rules for the processing – particularly sharing – of data but rather it constitutes an integral base layer framework for enabling data, particularly non-personal, sharing across different actors and industries. In this sense, the DA pushes for rules to: (i) govern business-to-consumer and business-to-business data sharing, (ii) ensure that data is made available by data holders, (iii) address anticompetitive contractual provisions between firms regarding data access, (iv) facilitate private data sharing to public bodies, (v) switch between data processing services, (vi) allow international data transfer, and (vii) safeguard interoperability between data spaces.

When it comes to personal data, Recital 24 indicates that any personal data processing should be governed by the GDPR. However, as personal and non-personal data become more intertwined categories, Recital 30 gives some clarification regarding how the interpretation of the cumulative protection should be understood, but both the EDPB and the EDPS call for further clarification on the interplay with the GDPR. In this respect, if the user is also a data subject, then it would also be entitled to be protected under the DA as well as under the GDPR.

It is possible to identify that the DA also relies heavily on voluntary decisions, in this case in the form of contractual agreements, to enable data sharing. In this respect, this would lead to a very similar situation as with the Payment Services Directive 2 and the role of contractual consent to enable data sharing. As the DA is intended to supplement the GDPR with data-sharing specific duties and obligations, we can find provisions, such as its Art. 3.2, that provide for further transparency that could contribute toward properly informed consent. Moreover, Art. 28 requires the use of standards on different components to secure the interoperability between datasets. This would allow users to move around different data processing services upon their decision (consent).

IV. Towards a technologically assisted consent?

While each new legal instrument has a distinct purpose and deals with processing personal data differently, there is a common pattern across them: the reliance on consent as the primary legal basis. However, is this a sensible bet? Not just in the realm of data protection but in other fields, such as consumer protection, the capacity of individuals to make choices on their own in the digital economy has been put under the spotlight for quite some time.

Do this mean that consent was the wrong choice to govern personal data flows in the platform economy? Would it have been more sensible for the European Union to limit together certain practices and put more stringent limitations on how (personal) data can be processed by platforms?

While some practices have been partially limited, such as under the DMA, many others are still possible and even encouraged by other EU policy efforts, particularly data sharing and re-use, if consent has been validly collected. To help obtain such a legal basis, these new regulations and other related legislation provide for two tools, one technological and one organizational, that could help in this endeavor: the development of personal data spaces and the assistance of the data subject.

1. Can consent address power asymmetries?

One could argue that the Commission’s vision for the data economy in these new laws is grounded on the idea of empowering data subjects, hence the choice of consent, to grant further control against data processing practices by platforms deemed unfair to them, whether it is how platforms decide which content gets taken down or if they are being influenced regarding certain online search ranking results.

While certain practices have been limited, consent can enable them back, such as in the case of the DMA. However, academics, industry practitioners, and civil society members had raised their concerns over the fact that with just one click on an ‘ok’/I accept button, the right to data protection could be vandalized by abusive practices once again. In this sense, it was argued that consent is not an adequate tool to balance digital markets. Nevertheless, it is also possible to argue that the very same DMA has provisions to prevent this. In this sense, not consenting should be as easy as consenting, and gatekeepers should seek consent using user-friendly schemes and avoid the adoption of deploying dark patterns to obtain consent.

Out of all the reviewed instruments, the DGA provides a considerable number of provisions to reflect on the use of consent as a legal basis to enable the envisaged data-sharing environment by the Commission. Starting with data held by public bodies, the DGA pushes for the use of consent when other bases fail to allow secondary data processing and it requires public bodies to help in the quest to obtain consent, for which they are allowed to charge a fee. Regarding this collaboration to obtain consent, public bodies should act as intermediaries, mainly through a single information point, between data subjects and re-users and, particularly when pseudonymized personal data is involved, should en-

---

20 Chapter II DA.  
21 Chapter III DA.  
22 Chapter IV DA.  
23 Chapter V DA.  
24 Chapter VI DA.  
25 Chapter VII DA.  
26 Recital 24 DA.  
28 Recital 30 DA.  
29 Joint Opinion 02/2022 on the Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act) [n 12].  
30 Art. 3.2 and 4.6 DA.  
32 Art. 5.2. in fine and 6.10 DMA.  
33 F. 1. 2.  
34 Art. 5.2. in fine and 6.10 DMA.  
37 Recital 37 DMA.  
38 Art. 13.5 DMA.  
39 Art. 5.6 DMA.  
40 Recital 26 DMA.  
41 Aida Ponce del Castillo, ‘Chapter 4 Europe’s Digital Agenda: People-Centric, Data-Centric or Both?’, Social policy in the European Union: state of play 2021. Re-emerging social ambitions as the EU recovers from the pandemic (European Trade Union Institute and European Social Observatory 2021).  
42 Art. 6.5. (f) DGA.  
43 Art. 5.6. (j) DGA.  
44 Recital 37 DMA.  
45 Recital 37 DMA.  
46 Recital 26 DA.  
47 Recital 26 DA.
sure that data subjects’ contact information is not passed along to the potential re-users.91

Moreover, regarding data altruism organizations, they have to ‘(...) provide tools for obtaining consent from data subjects (...) also provide tools for easy withdrawal of such consent (...)’.92 Besides this, if they provide access to third parties, they also have to facilitate tools for securing consent.93 In this respect, the Commission can develop templates for ease of use between services for the benefit of the data subject.94

While limited to the context of the DGA, the European data altruism consent form might provide some direction on this to foster ‘(...) trust and bring additional legal certainty and user-friendliness to the process of granting and withdrawing consent’.95 In particular, this instrument would be handy as it is already foreseen that it should have a modular approach.96

2. Mapping how data is used: the role of personal data spaces

The first component in the Commission’s plan to enhance consent in the data economy is the development of personal data spaces and associated technologies. Little scholarly work has been done around data spaces, mostly given their slow policy and regulatory development.97

One of the earliest references to them can be traced back to a 2014 policy document: ‘Towards a thriving data-driven economy’.99 In this document, personal data spaces were conceptualized as a form of personal information management system,100 that would serve data subjects in deciding how their information could be shared. This approach was later changed towards a vision of data spaces as the data sharing infrastructure for both personal and non-personal data that ensures a high degree of interoperability across and within them, where the main decision-makers would be data controllers, with the data subjects’ consent.101 So far, the Commission only made public a proposal for the EHDS. It is based around data subjects deciding how their personal (health, in this case) data circulates in the European Union and beyond.102

Considering that data spaces are another piece on the regulatory agenda, how are data spaces connected with this new regulatory package for the management of personal data? We can start with the instruments that provide a lesser number of connections. Firstly, both the DMA and the DSA provide no reference to them so we can easily leave them aside. In contrast, the DA contains considerable references to data spaces. While it focuses primarily on non-personal data, it does provide a whole chapter on ensuring that data spaces are interoperable.103

Finally, we can discuss the link with the DGA. As with the DA, there are plenty of references to data spaces in this regulation. Under the DGA, the new data governance schemes introduced are intended to help data subjects in navigating data spaces and the broader data economy. These third parties would assist them in handling their personal data, either directly in the case of data intermediation services –particularly data cooperatives–,104 or indirectly in the case of data altruism.105 We will return to this issue of assisting the data subject in the following section.

The DGA also intends to engage with personal data spaces, as a form of personal information management system. In this sense, data intermediaries would facilitate that data is processed on users’ devices rather than being communicated to a data controller to be processed on its premises.106 Under this approach, a data subject would even be in a better position than in regular data spaces as its personal information would have never been taken out of its control, and access to it can easily and effectively be revoked when desired or necessary.

Personal data spaces are expected to be cover in the update to Regulation 910/2014 (eIDAS), commonly known as eIDAS2.107 While eIDAS 2 involves a considerable number of amendments to the original regulation, its main novelty resides in the introduction of the European Digital Identity Wallet, which is defined as ‘(...) a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service (...)’.108

These personal data spaces can provide support in managing consent and privacy preferences for data subjects using personal data wallets. Some Member States have moved forward by providing a regulatory framework to these solutions, such as Germany,109 but this would constitute a considerable improvement to secure legal certainty at a EU-level. In this respect, there are already technical developments in the field, such as SOLID, and some scholars have already provided their input into them.110 However, it is possible that under this premise, data subjects are even more overloaded with data-related decisions and the protections of GDPR are watered down under false promises of more user control.111

---

91 Recital 15 DGA.
92 Art. 21.6 DGA.
93 Art. 21.6 DGA.
94 Recital 52, and Arts. 22.1. (a) and 25 DGA.
95 Recital 52 and Art. 25 DGA.
96 Art. 25.2 DGA.
97 For examples of this, see Anastasiya Kiseleva and Paul de Hert, ‘Creating a European Health Data Space: Obstacles in Four Key Legal Areas’ (2021) 5 European Pharmaceutical Law Review (EPLR) 21; Giovanni Comandé and Giulia Schneider, ‘It’s Time. Leveraging The GDPR to Shift the Balance Towards Research-Friendly EU Data Spaces’ [2022] Common Market Law Review 34.
98 As of July 2022, the Commission only published a proposal for the creation of a single data space -the EHDS- out of the nine envisaged data spaces.
99 ‘Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions “Towards a Thriving Data-Driven Economy”’ [n 16].
101 ‘Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions “Towards a Common European Data Space”’ [n 16]; ‘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’ [n 1].
102 Art. 3.5. (a) and 3.8 EHDS.
103 Chapter VIII DA.
104 Recital 27, 30, 31, 32, 33 and 34 DGA.
105 Recital 45 DGA.
106 Recital 30 DGA.
108 Art. 1. (3). (i) eIDAS 2.
109 § 26 TTDG
Ultimately, a combination of both kinds of data spaces would seem to fit within the Commission’s agenda as the latter mature into more robust forms of personal information management systems. In particular, as consent has been given a central role in these data-intensive, more user control is necessary and these technological tools can deliver this, particularly if the whole data ecosystem is interconnected as interoperable as envisaged by the EU data spaces policy.

While the effective development of these data spaces, in both forms, is still a pending issue, certain developments in this field would seem inclined to allow for an easy map out of how certain data, in this case about an individual, would be distributed in the field. This would, in turn, allow the data subject to relatively quickly assess how its data has circulated.

3. Helping data subjects making online choices

While data spaces would provide technical support to map out how personal data is used, it is possible to identify the emergence of certain assistance duties to help data subjects in providing their consent to those data processing operations, particular sharing. As noted before, the very idea of a reasonable and capable data subject that can master every single aspect of how its personal data is used is far behind. In this sense, data subjects would need help in understanding complex documents; other fields, such as financial services, are also developing a similar duty.

Of all the reviewed instruments, only the DGA has provisions for this. Data subjects can expect to receive further guidance on data processing conditions through guidance, particularly through data cooperatives; these would help data subjects ‘in making informed choices before consenting to data processing.’ While not expressly included in the DGA’s provisions, the possibility of assisting can also be performed by other kinds of data intermediary services. This task would also be expected from the competent public bodies under the DGA for the re-use of public data when helping potential data re-users.

However, there is a major shortcoming to the reliance on these entities: the fact that data subjects need to actively become a member of these to receive their ‘protection’. It is highly unlikely that, for example, these data cooperatives would rely on a ‘brick-and-mortar’ infrastructure to provide help but rather leverage on technological means to reach out to their users according to their needs. Nevertheless, data subjects would not be entitled to this level of assistance unless they voluntarily agree to be part of any of them. The DGA does not provide more rules for this novel approach to enhancing consent and it is only possible to wonder about its details and concrete implications, such as whether the data cooperative can be held liable for damages resulting from the advice.

Besides this, then we have the question of whether the personal data included in the data cooperative is held by the cooperative on an aggregate basis or rather the data subject is still in charge of it. This discussion, particularly around the very idea of data com-

4. Can we wait for this bet to pay off?

Assisting consent with existing frameworks

Ultimately, the real question at the table is whether as we wait for all these pieces to fall together, data subjects would not be at risk from current practices that are not addressed adequately due to unclear regulation, lack of enforcement, or conflicts between who must make what decisions when it comes to the regulatory framework. The infancy of these tools was acknowledged in the policy document ‘A European strategy for data’, but the bet was placed on the table anyways.

As analyzed, consent is expected to serve as the primary legal basis to ensure that data sharing and (re-)use is fairer towards data subjects. This gamble could pay off with clear benefits for data subjects across Europe and potentially beyond it given the Brussels effect. However, the losses can also be quite high if consent falls again in its existing defects and shortcomings, as feared by the mentioned concerns on DMA’s Art. 5.1. (a).

The path of assisting the data subject can also be explored under the current framework provided exclusively by the GDPR. For example, as mentioned above, the financial services industry already has in place a similar ‘assist the client’ obligation within certain regulations. This duty is set around the idea that power asymmetries between different parties in a regulatory framework based around risk management can be addressed by complete and helpful transparency from the stronger party to the other. For example, a bank should explain its client the concrete consequences from taking up a new loan, even if the client is provided with all the relevant information in an adapted format.

While a specific provision as this does not exist in the GDPR, the same logic can be transposed and applied given the imbalances between data controllers and data subjects, the presence of a risk-based approach, the enabling role of consent, and the possibility of unforeseen consequences for the data subject. Issues such as whether this consent would be valid under GDPR, if the data controller can be trusted with this, or the benefits of bright patterns to guide data subjects are unanswered question on this. This discussion might also prove beneficial for other proposed rules that rely considerably on consent, such as the ePrivacy Regulation proposal.

---

112 ‘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’ [n 1] 10.
114 Recital 31 and Art. 2. [15] DGA.
115 Recital 30 DGA.
116 Recital 26 DGA.
117 ‘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’ [n 1] 10.
119 Busch, Colaert and Helleringer (n 112).
V. Conclusions

Consent’s requirements, besides being free and informed, demand both specificity and unambiguity on the intended data processing activities. However, data subjects are expected to be exposed to a considerable number of decisions making situations under this economic model based on the intensive use of (personal) data.

The new regulatory package has selected consent as its primary champion for different issues, such as to enable back the online advertising business model in the DMA or to facilitate data sharing under the DGA. At the same time, these new rules propose the adoption of new data governance schemes to help data subjects in managing their personal data in a more participative manner, such as through data cooperatives. In this sense, the regulatory package is quite ambitious and tries to deliver on its objectives by providing certain tools to enhance consent according to these demands.

In the meantime, until these tools are developed and deployed, how can we secure consent as required by the GDPR? Consent can only be (i) free, (ii) informed, (iii) specific, and (iv) unambiguous if data subjects understand what they are consenting to. In this respect, transparency plays a fundamental role. However, current practices fail to achieve their desired outcome. The path of the ‘assisted’ consent might prove worth exploring, even without an express regulatory framework for it beyond the general provisions of the GDPR. Under this, gatekeepers should, beyond providing a privacy notice, explain the consequences in an individualized manner to data subjects vis-à-vis financial services providers must guide and help consumers in making choices relative to their investment portfolios or credit applications.