BRUSSELS PRIVACY HUB

WORKING PAPER

VOL. 11 • N° 2 • JULY 2025

THE FUTURE OF DATA GOVERNANCE IN THE EU:

A Response to The Call for Evidence on the Data Union Strategy Initiative

By Andrés Chomczyk Penedo*, Bárbara da Rosa Lazarotto*, Pablo Trigo Kramcsak*, and Sophie Stalla-Bourdillon*

*Postdoctoral researcher at the Institute of Law and Technology of the Universitat Autònoma de Barcelona; affiliated researcher at the LSTS, Vrije Universiteit Brussel, Fellow of the Brussels Privacy Hub.

*PhD Researcher at LSTS, Vrije Universiteit Brussel, Managing Director of the Brussels Privacy Hub.

*PhD Researcher at LSTS, Vrije Universiteit Brussel, Fellow of the Brussels Privacy Hub.

*Co-Director of the Brussels Privacy Hub, LSTS, Vrije Universiteit Brussel.

Contents

1 Introduction

The CfE supporting the development of the Data Union Strategy starts its analysis by stating that *"[t]he 2020 EU data strategy has yielded some results: the creation of common European data spaces as decentralized frameworks for the sovereign sharing and pooling of data by companies, e.g. with the help of data intermediation services regulated under the Data Governance Act; new rights of access to and sharing of industrial data under the Data Act; and health data under the European Health Data Space Regulation*."[1] While the second staff working document on data spaces highlights several developments, these results are thus not considered to be sufficient.[2]

The AI Continent Action Plan (the "AI Plan"), which includes the Data Union Strategy as a key milestone, proposes a set of actions to move forward.[3] It announces that the data space structure will be enhanced by establishing data labs that will serve a variety of functions.[4] Data Labs will facilitate access to common European data spaces and offer services like data cleaning, enrichment, technical tools, and cross-sector interoperability. They may also support data pooling in compliance with antitrust rules, in an attempt to transform fragmented data into a resource usable for AI development, leveraging data intermediation services under the Data Governance Act (DGA).[5]

In addition, the AI Plan presents the Data Union Strategy as an instrument that will be developed to strengthen *"the EU's data ecosystem by enhancing interoperability and data availability across sectors, to respond to the scarcity of robust and high-quality data for the training and validation of AI models. It will aim to better align data policies with the needs of businesses, the public sector, and society, while fostering a trustworthy environment for data sharing."*[6] To meet this goal, the AI Plan adds that *"[p]articular attention will be given to streamlining existing data legislation to reduce complexity and administrative burden and to ensure that data governance structures are efficient*

[1] European Commission, 'Call for Evidence for a European Data Union Strategy' (2025) Ares (2025)4163996 1 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14541-European-Data-Union-Strategy_en>, accessed 17 June 2025.

[2] The second staff working document released in January 2024 provides an overview of the current status of the common European data spaces following the first staff working document released in February 2022. It concludes by observing that "it is evident that the pace of development varies significantly among data spaces, leaving a considerable amount of work yet to be completed." European Commission, 'Commission Staff Working Document on Common European Data Spaces' (2024) SWD(2024) 21 final 52 <https://digital-strategy.ec.europa.eu/en/library/second-staff-working-document-data spaces#:~:text=This%20Second%20staff%20working%20document%2C%20published%20in%20January,current%20status%20of%20the%20common%20European%20data%20spaces.>, accessed 17 June 2025.

[3] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The AI Continent Action Plan' (2025) COM(2025) 165 final <https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan>, accessed 17 June 2025.

[4] Ibid.

[5] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) OJ L 152, 3.6.2022, p. 1–44.

[6] ibid.

and effective, based on an inclusive process that takes into account applicable copyright legislation."[7] The simplification agenda appears, therefore, driven by the will to guarantee "*efficient and effective data governance structures.*" This motivation is echoed in the CfE, which frames simplification as a means to enhance the coherence of existing instruments. The aim, it notes, is "*to make the instruments work together in the best way for an effective data economy, including effective governance mechanisms*."[8]

Although the notion of data governance is multifaceted and context-dependent,[9] for the purpose of this CfE, we understand data governance structures or mechanisms in a regulatory context to mean a system of rules, principles, and standards governing the management, access, and sharing of data across different actors and sectors.[10] Such a normative system comprises both horizontal and vertical rules. By way of example, the Data Act (DA)[11] puts forward "*a general approach to assigning rights regarding access to and the use of data*"[12] with a view "*to realise the important economic benefits of data, including by way of data sharing on the basis of voluntary agreements and the development of data-driven value creation by Union enterprises.*"[13] On the other hand, the European Health Data Space Regulation (EHDS)[14] aims to set up among other things "*a consistent and efficient framework for the reuse of natural persons' health data for research, innovation, policymaking and regulatory activities*."[15] In this context, data spaces, from healthcare to finance, thus exemplifies such data governance structures or mechanisms.[16] Recital 5 of the DGA offers a grounding for such a normative system. Under Recital 5 DGA, the regulatory goals should be to ensure "*control by data subjects and data holders over data that relates to them*," and to "*address other barriers to a well-functioning and competitive data-driven economy*." The means to achieve these goals include in particular facilitating the exercise of data subject rights, which are part of the

[7] Ibid.
[8] Call for Evidence for a European Data Union Strategy 2.
[9] Haleh Asgarinia, Andrés Chomczyk Penedo, Beatriz Esteves, & Dave Lewis,'"Who Should I Trust with My Data?" Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies' (2023) 14(7) Information, 351, https://doi.org/10.3390/info14070351.
[10] Note that the EHDS only refers to a governance framework without defining this term. See Article 1(1) EHDS.
[11] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) OJ L, 2023/2854, 22.12.2023.
[12] Recital 6 DA.
[13] Recital 6 DA. The DA is horizontal in the sense that Chapter II and III applies to connected products in general.
[14] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 OJ L, 2025/327, 5.3.2025.
[15] Recital 110 EHDS.
[16] In this sense, Chomczyk Penedo argues that a data governance mechanism is one main characteristic of data spaces, based on an analysis of their inception policy documents (see Andrés Chomczyk Penedo, 'The Regulation of Data Spaces under the EU Data Strategy: Towards the 'Act-ification' of the Fifth European Freedom for Data?' (2024) 15(1) European Journal of Law and Technology.

GDPR acquis, facilitating the reuse of certain categories of data held by public sector bodies and the supply of data intermediation and data altruism services, which drive key provisions of the DGA.[17] This response focuses upon the first prong of the second objective underlined in the CfE, i.e., simplification through streamlining existing rules. It seeks to highlight **five challenging points** emerging from the European Union (EU)'s regulatory approach to data governance, analysed through the lens of data protection law. Rather than calling for a reopening of the GDPR, this response underscores that it is the absence of an overarching conceptual framework underpinning post-GDPR regulations that generates interpretative tensions and fosters ambiguity. To address this, it advocates for a more integrated conceptual framework and a clearer articulation of the interplay between the GDPR and subsequent regulations, with a view to preserving the integrity of the GDPR acquis.

2 The terminology used in post-GDPR regulations is intricate

The General Data Protection Regulation (GDPR)22 stands as a foundational pillar of the EU's data governance framework.[18] Its strength lies in the internal coherence of its conceptual architecture: key notions such as *personal data, processing, controller, data subject, and consent* are tightly interconnected and grounded in a rich body of jurisprudence and regulatory guidance. This internal consistency has fostered a shared vocabulary across public and private actors at an EU level, contributing to a relatively stable and predictable regulatory environment in the Digital Single Market.[19] In this context, consistency in terminology is not merely formalistic: it underpins legal certainty, facilitates enforcement, and ensures that fundamental rights are meaningfully protected in practice across the EU.

[17] Recital 5 DA.

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

[19] While reliance on a regulation rather than a directive has significantly facilitated this trend, three important nuances need to be introduced. Firstly, we acknowledge that the GDPR does allow Member States some margin for maneuver when it comes to a selection of particular topics, such as for example the research exemption provided for Article 89 GDPR (see, for example, Denise Amram, 'Building up the "Accountable Ulysses" Model: The Impact of GDPR and National Implementations, Ethics, and Health-Data Research: Comparative Remarks' (2020) 37 Computer Law & Security Review 105413). Secondly, we also concede that the intervention of different "hands' in the process of drafting data- related legal rules might also contribute to the terminology issues identified below (see Magdalena Brewczyńska, 'Between Legitimacy and Lawfulness: In Search of Rationality and Consistency in EU Data Protection' (2023) 9(2) European Data Protection Law Review 112 https://doi.org/10.21552/edpl/2023/2/6). And thirdly, current enforcement practices across supervisory authorities have not been equal across the board (see Giulia Gentile and Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' (2022) 71(4) International and Comparative Law Quarterly 799).

In contrast, recent legislative initiatives, including the DGA, the DA, the Digital Markets Act (DMA)[20] and the Digital Services Act (DSA),[21] but also the emerging sector-specific data spaces regulations, e.g., for healthcare or finance, introduce specific legal terminologies and conceptual frameworks to pursue their respective policy objectives. While some instruments rely on previously harmonised notions, others deploy novel or bespoke terms, likely in an attempt to minimise conflicts with the existing acquis or to simply build on top. Although these instruments seek to complement the GDPR by addressing areas arguably beyond its scope—particularly through the introduction of new rights—the lack of clear alignment with established definitions engenders significant substantive ambiguity. This, in turn, is likely to create legal complexity at the implementation stage and undermine the coherence of the broader EU data strategy.

Subtle yet significant divergences between concepts such as *portability* under Article 20 GDPR, *access* and *making available* under Articles 4 and 5 DA, *switching* under Chapter VI DA, *portability* under Article 6(9) and (10) DMA underscore the lack of conceptual alignment across instruments, although the intention to broaden the domain and effect of Article 20 GDPR is to be welcome. Seemingly-wide concepts such as *data holders* defined either through the right to grant access or to share data27 or to use and make available data[22] generate ambiguities, particularly when overlaps between related concepts are not systematically tracked and unpacked.[23] More generally, the proliferation of new actor categories such as *data users, users of connected products*, *data recipients*, and *data intermediation service providers*, without an overarching taxonomy, deepens the fragmentation of the regulatory landscape.

To illustrate the intricacies of the terminology, let's take an example, which could be represented in part with Figure 1. The owner of a connected product, such as a virtual assistant, is a *user* under Art. 2(12) DA, but could also be labelled a *data user* under Article 2(9) DGA, although the DA does not introduce such a term. A *user* under the DA may or may not be a *data subject* under the GDPR, as users can also be legal persons (e.g., employers of data subjects) and data subjects within the meaning of Article 4(1) GDPR only cover natural persons. Under the DA, a user may either access data directly from the product or request it from the *data holder*. A *user* can also request the *data*

[20] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L 265, 12.10.2022, p. 1–66.
[21] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, p. 1–102.
[22] Article 2(8) DGA.
[23] For example, under the DA a data holder is not necessarily a manufacturer of a connected product, which would suggest that a user of a connected product could also be a data holder.

holder to share data with a third party under Article 5(1) DA, which becomes a *data recipient* under the DA. A *third party* under the DA would then also be considered a *recipient* under the GDPR, but only if personal data is involved, just like a *user* of a connected product who is not a *data subject* (e.g., the employer of the data subject). Nothing in the DA appears to prevent a *data recipient* under the DA from also being classified as a data holder under the DA, as the category of *data holder* under the DA is broader than that of product manufacturer. A *data holder* under the DA seems however to exclude processors within the meaning of the GDPR,[24] although processors have the right to user personal data within the bounds of contractual limitations.[25]

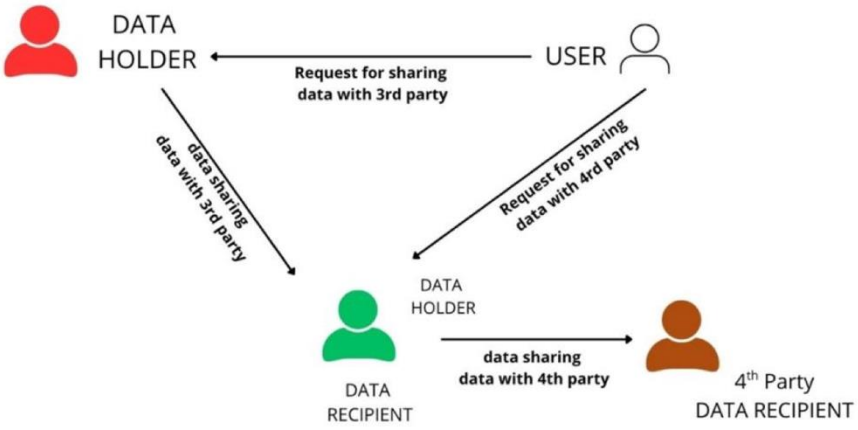

Figure 1: A relatively small chain of actors under the DA

Similar issues arise as regards the distinction between consent, as developed under the GDPR,[26] and permission mechanisms introduced for a variety of use cases, e.g. non- personal data reuse under Article 2(6) DGA, or data analysis to infer certain characteristics of data recipients under Article 5(6) DA. These operate under different normative assumptions and are governed by different safeguards, yet the boundaries between personal and non-personal data are often fluid, as explained below under point 3.

The concept of permission has been introduced in Financial Data Access (FiDA)[27] and Payment Services Regulation (PSR)[28] proposals, in an attempt to streamline the conceptual arsenal of the client-facing European Financial Data Space (EFDS). Such an introduction finds its roots in the earlier

[24] Recital 22 DA.
[25] It should be noted, however, that many actors operate as both processors and controllers, as data flows between the same parties often serve a variety of processing purposes.
[26] See Article 4(11) GDPR.
[27] Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554COM/2023/360 final.
[28] Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 COM/2023/367 final.

Payment Services Directive 2 (PSD2),[29] which established open banking, and relied on the notion of 'explicit consent' instead.[30] In this respect, Recital 69 of the PSR proposal expressly acknowledges that "[t]he parallel use of the term 'explicit consent' in Directive (EU) 2015/2366 and Regulation (EU) 2016/679 of the European Parliament and of the Council has led to misinterpretations." The term permission is therefore introduced to replace the concept of *explicit consent*.[31] It is also clarified in the PSR proposal that characterising a permission is not necessarily associated with the notion of consent under Article 6 GDPR.[32] In other words, the whole catalogue of GDPR legal bases is, in principle, available to support permissions within the meaning of PSR, just like the FiDA proposal acknowledges it in Recitals 10 and 22 but without mentioning past interpretative issues.[33] Although the concepts of EFDS permission and GDPR consent now appear distinct, the EU concept of permission and national concepts of contractual acceptance are likely to overlap.[34]

One other key set of concepts, which is involved in legitimising data reuse comprises that of general interest found for example in Article 2(16) DGA, and the concept of public interest found in various provisions of the GDPR, e.g., Article 6(1)(e) or the EHDS, e.g., Article 55(5). The extent to which these concepts overlap remains unclear.

Taken together, these developments reflect a broader shift toward a layered regulatory landscape that is, at times, extremely intricate, if not inconsistent. The DA, for instance, illustrates this tendency in its treatment of subsidiarity and the pre-emptive effect on national legislation.[35] The increasing use of aspirational or policy-oriented terminology, often lacking firm conceptual grounding, threatens to erode legal clarity, disrupt regulatory coherence, and has the potential to weaken the effective protection of data subjects' rights.

---

[29] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC OJ L 337, 23.12.2015, p. 35–127.

[30] For an in-depth analysis, see Federico Ferretti, 'Open Banking: Gordian Legal Knots in the Uncomfortable Cohabitation between the PSD2 and the GDPR' (2022) 30(1) *European Review of Private Law*.

[31] See in particular Article 95(2) PSD2 which refers to explicit consent in an article devoted to data protection.

[32] Recital 69 PSR proposal.

[33] Andrés Chomczyk Penedo, 'The Meta v. Bundeskartellamt Judgment and its Impact on a Consent-Based European Financial Data Space' [A People's Financial Regulation? Competition Law and Economics in the Financial Services Sector, Tilburg University, 13 June 2025].

[34] The EDPB argues that explicit consent under PSD2 is contractual in nature. EDPB, Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR. Version 2.0, 15 December 2020, p. 13-15, <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_en>, accessed 17 July 2025. See also Eugerta Muçi, 'Open Banking in the EU: A Consumer Dystopia or Utopia?' in K Prifti, E Demir, J Krämer, K Heine and E. Stamhuis (eds), Digital Governance: Confronting the Challenges Posed by Artificial Intelligence (1st edn, vol 39, TMC Asser Press 2024) 89 https://doi.org/10.1007/978-94-6265-639-0_5.

[35] See Article 1(5) DA. See also Jan Krämer and others, Towards a Balanced EU Data Act (CERRE, March 2023), <https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf, accessed 9 July 2025.

3 Data Spaces are bespoke data sharing ecosystems, with bespoke data governance structures, even when set up through regulation

As briefly noted above, sector-specific regulations have been or are in the process of being adopted for common European data spaces. This thus means that, at this time, most data spaces are currently not specifically set up through regulation, but rather under the Digital Europe programme, as noted in the second staff working document on data spaces.[36] For these non-common data spaces, despite the setting forth of a Data Space Support Centre[37] funded by the Commission, which is supposed to help them achieve legal compliance with its toolbox,[38] there does not seem to be ad hoc and detailed legal assessments.

As regards common European data spaces, it remains unclear whether the EU lawmaker has successfully resolved the interplay between the bespoke data governance framework established by sector-specific regulation and the GDPR. As hinted in the first section, a first concern lies in the reliance on bespoke definitions, which are not easily aligned with the existing acquis. To add another example, the FiDA proposal limits who can be data user to a selected cohort of financial institutions, as detailed in its Article 3(6). The same is true for the notion of data holder, under Article 3(5). At the same time, the PSR proposal does not leverage this terminology but relies on terms introduced in PSD2 for open banking.[39]

Second, the legal regime to facilitate the sharing and repurposing of data created by the DGA is not really leveraged within the bespoke data space regulatory frameworks. In this respect, the EHDS ignores the two main sets of rules laid down in the DGA, i.e., rules concerning data intermediation services, and data altruism, and introduces bespoke 'health data intermediation entities, which are expressly distinguished from data intermediation services under the DGA, as noted in Recital 59 EHDS. As for the EFDS, it refers to data intermediation services in the FiDA proposal, but not in the PSR proposal, for one use case: the provision of the permission dashboard, as noted in Recital 21 of the FiDA proposal. More generally, trust is supposed to be achieved through the setting forth of a

[36] See Commission Staff Working Document on Common European Data Spaces.
[37] https://dssc.eu/, accessed 17 June 2025.
[38] https://dssc.eu/space/BVE2/1071253931/Regulatory+Compliance, accessed 17 June 2025.
[39] See Articles 3(19), (22) and (23) PSR proposal.

bespoke regime for financial information service providers acting as data users per Article 3(6)-(7) of the FiDA proposal.

Third, while it might be necessary to develop bespoke rules for each sector, it is unclear whether an interoperability requirement found in the DA or initiatives, like Simpl,[40] to develop a common technical infrastructure will be enough to lay the foundation for an EU Data Union. On a regulatory front, ambiguities could also emerge from the fact that new rules may appear to establish competing data access regimes—for example, the DA and the EHDS with respect to data generated by medical devices.

4 The anonymisation approach emerging in post-GDPR regulations is not clearly articulated

An analysis of various post-GDPR regulations reveals a lack of clarity as to whether the drafters adopted a consistent approach to anonymising personal data. Yet, such consistency is crucial, as anonymisation is regarded as a key or (even simply) relevant safeguard for enabling data reuse.

To start with, the language used in these regulations does not align with the terminology developed by the European Data Protection Board (EDPB)'s predecessor in its first opinion on *anonymisation techniques* under the Data Protection Directive.[41] In this opinion, the expression *anonymisation techniques* is used as an umbrella term that covers a wide range of techniques, including k-anonymisation and differential privacy, and anonymisation as a legal concept is grounded on the means test. From this framing, it should then be clear that leveraging an anonymisation technique does not necessarily imply that the legal test for anonymisation has been met. In order to meet the legal standard for anonymisation, the EDPB's predecessor had suggested that two routes are potentially open: addressing three re-identification risks (i.e., singling out, linkability and inference) or performing a thorough risk analysis and implementing a diverse set of controls, including data and context controls.[42]

[40] See https://simpl-programme.ec.europa.eu/, accessed 16 July 2025.
[41] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) WP216 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, accessed 6 July 2025.
[42] See ibid 26. For a conceptualisation of data and context controls see Sophie Stalla-Bourdillon and Alfred Rossi, 'Aggregation, Synthesisation and Anonymisation: A Call for a Risk-Based Assessment of Anonymisation Approaches' in Dara Hallinan, Ronald Leenes and Paul De Hert (eds), Data Protection and Privacy: Data Protection and Artificial Intelligence (Hart Publishing 2021).

By way of example, Recital 7 DGA appears to conflate the legal concept of anonymisation with a broad spectrum of anonymisation techniques, which differ considerably in the degree of privacy protection they afford: "differential privacy, generalisation, suppression and randomisation, the use of synthetic data or similar methods and other state-of-the-art privacy-preserving methods."

Moreover, it remains unclear whether the DGA and the DA are based on the assumption that data status can be compartmentalised—namely, that the same transformed data could be considered personal in the hands of the original data holder or provider as it still holds untransformed data, and yet be regarded as anonymised when processed by the data user or data recipient in the light of the context controls applied to the data environments.[43] A purposive reading of both the DGA and the DA suggests that the compartmentalisation of data status may be considered possible; otherwise, anonymised data would be exceedingly rare, and presenting anonymisation as a meaningful option for data sharing[44] would appear largely incoherent. Feedback loops—understood as iterative processes in which insights generated from transformed data are used to inform or influence the handling, interpretation, or further processing of the original, untransformed data—should nonetheless prompt a more nuanced assessment and arguably preclude the compartmentalisation of data status.[45]

Looking at the CJEU case law and guidance produced by the EDPB so far, it may be possible to develop an approach to anonymisation that would align with the concepts and methods used on the ground by de-identification experts, while preserving a functional definition of personal data which is needed to govern processing practices such as profiling.[46] Such an approach, however, entails acknowledging that the secondary purposes (for which the anonymised data will ultimately be used) must be legitimate and that anonymisation in itself is not a purpose. This is because, if 'anonymised data' is understood to exist in practice, some level of residual re-identification risk is likely to persist, while individuals lose control over the data pertaining to them until the point at which re-identification occurs.

Neither the DGA nor the DA address the concept of purpose or emphasise its significance, although both instruments, as mentioned above, are intended to be without prejudice to the GDPR.[47] What

[43] It is worth noting that the EDPB's predecessor on this point has not been very clear. See Sophie Stalla-Bourdillon, 'Identifiability as a Data Risk: Is a Uniform Approach to Anonymisation About to Emerge in the EU?' [2025] European Journal of Risk Regulation 1.
[44] See e.g., Article 5 DGA, and Article 18(4) DA.
[45] See Stalla-Bourdillon.
[46] ibid.
[47] See Recital 4 and Article 1(3) DGA and Recital 7 and Article 1(5) DA.

is more, both data and model information are relevant for constructing an approach to personal data anonymisation under the GDPR as explained by the EDPB itself.[48] From the EDPB's analysis, it should be clear that considering the downstream processing use case, including model training and possibly even model deployment, appear to be relevant for deriving the legal effects of the so-called anonymisation technique implemented within a particular environment.[49] Yet, none of the newly-introduced data reuse regimes that seem to give a role to anonymisation as an appropriate safeguard for reuse makes this explicit.

5 New data access regimes set forth in post-GDPR regulations are heterogeneous

When analysing new data sharing and reuse regimes in the light of Article 6 GDPR, which sets forth an exhaustive list of legal bases for processing personal data, these provisions appear lacking clarity for their operationalisation. They are often broadly defined with no references to covered subsequent processing purposes in the sense of the GDPR, although the EHDS does include a list of high-level in scope purposes and a list of high-level prohibited purposes. While the EFDS, particularly under the FiDA proposal, introduces additional concepts, such as data use perimeter[50] and data sharing schemes,[51] their precise meaning remains uncertain at this point.[52] Further analysis is thus required to identify the most adequate legal basis for reuse.

In some cases, the regulatory framework appears even more shallow in that to make the data reuse regime function, a bespoke legal basis needs to be adopted at the national level. This is the case for the DGA. The DGA thus only focuses on outlining the role of the public sector body when a legal basis exists.[53] The DGA even goes quite far in this regard as if no bespoke legal basis exists at the national level it imposes upon public sector body an obligation to "make best efforts, in accordance

[48] EDPB, 'Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models' (2024) Opinion of the Board (Art 64), <https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf>, accessed 6 June 2025.
[49] See Sophie Stalla-Bourdillon and Alfred Rossi, 'A Critical Assessment of EDPB Opinion 28/2024: Towards a Principle-
Based Approach to Innovation?' (2025) 25 Privacy and Data Protection.
[50] See Article 7 FiDA Proposal.
[51] See Title IV FiDA Proposal.
[52] The EDPB should contribute to guidelines produced by the European Banking Authority and the European Insurance and Occupational Pensions Authority on the notion of data use perimeter. See Article 7(4) FiDA Proposal.
[53] See Article 5 DGA.

with Union and national law, to provide assistance to potential re-users in seeking consent of the data subjects."[54] Such assistance should nonetheless ensure that consent meet the GDPR definition.

As a result, while formally compatibility is asserted, substantive alignment between the DGA and DA and the GDPR remains incomplete. Yet, the legal basis for processing data, must always be identified from the outset, prior to the actual processing, and must be communicated to the data subject.[55]

At this point, it is also important to stress that the proliferation of new scenarios for data (re)use, anchored in contractual obligations or sector-specific mandates, risks undermining the foundational principles of rights-based data governance under the GDPR, in particular if key distinctions are not clear prior to the operationalisation of the newly introduced data access regimes. By way of example, the data access regime under Chapter II of the DA, just like other data access regimes stacked on top of the GDPR, relies upon a fundamental distinction between the right to access data held by a data subject within the meaning of the GDPR and the right to access data held by an entity that is not the data subject within the meaning of the GDPR. This is because when the right holder is not the data subject, the exercise of the right must be conditional upon, among other things, the identification of an appropriate legal basis for access within the meaning of Article 6 GDPR.[56] Notably, when non-personal data is inextricably related with personal data, all data should be treated as personal data.[57]

From this fundamental distinction, several questions of interpretation arise. One in particular relates to whether the data holder needs to perform compliance checks upon the data recipient and vice and versa. The DA tries to solve the matter through its Article 8(5) DA, which provides that *"[d]ata holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or with their obligations under this Regulation or other applicable Union law or national legislation adopted in accordance with Union law*."

[54] Article 5(6)m DGA.
[55] EDPB, Guidelines 1/2024 on processing personal data based on Article 6(1)(f) GDPR, Adopted on 8 October 2024, <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf>, accessed 17 July 2025.
[56] See Articles 4(12) and 5(7) DA.
[57] This line of reasoning has been adopted by the CJEU in relation to special categories of personal data. See Meta v Bundeskartellamt [2023] CJEU C-252/21, ECLI:EU:C:2023:537 [88].

6 Although the GDPR remains a foundational layer, the interplay between GDPR and post-GDPR rights appears underdeveloped

What is clear from post-GDPR data regulations is that GDPR remains the foundational layer. This has direct implications for the way the newly-introduced rights should interact with already-existing GDPR rights, although these are not expressly articulated in detail in the regulations themselves. We illustrate the importance of this point by delving into two rights: the GDPR right to access and the GDPR right to object and their interplays with the DA and the EHDS.

6.1 The GDPR right to access

Article 15 GDPR is anchored in constitutional law, as the EU Charter of Fundamental Rights[58] expressly makes the right to access a fundamental right under Article 8(2).The GDPR right to data access is considered to be a cornerstone of EU data protection law,[59] and is closely related to other data subject rights, such as the right to rectification and erasure, the right to restriction of processing, the right to portability, and the right to object: it enables them.[60] By definition, the GDPR right to data access can only be exercised by the data subject.[61]

The GDPR right to access is grounded in contestability considerations.[62] Several related objectives are associated with contestability. The right to data access is often described as a means to enhance the transparency of data processing and allow data subjects to comprehend how their personal data is being processed and the consequences of this processing, and ultimately to give data subjects *control* over their personal data.[63]

On the other hand, the right to data access under the DA does not have a fundamental right foundation. It can be exercised by the user of a connected product or a recipient of related services, who may be a natural or legal person. This prerogative is driven by market fairness considerations. The same is true for its portability component.

[58] Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407.
[59] Orla Lynskey, The Foundations of EU Data Protection Law (Oxford University Press 2015) Ch 6.
[60] The full analysis of the right to data access is outside of the scope of this study. For a complete analysis, see Rene Mahieu, 'The right of access to personal data in the EU: a legal and empirical analysis' (PhD thesis, Vrije Universiteit Brussel 2023).
[61] Gabriela Zanfir-Fortuna, 'Article 15(1) "Right of access by the data subject"', in Christopher Kuner, Lee Bygrave, Christopher Docksey, and Laura Drechsler (eds.), The EU general data protection regulation: a commentary (Oxford University Press 2020).
[62] For a recent expression of the rationale underlying Article 15 see Dun & Bradstreet Austria GmbH CJEU C-204/22, ECLI:EU:C:2025:117. See also Recital 63 GDPR.
[63] Zanfir-Fortuna.

These considerations have direct implications for the scope of DA rights. The GDPR and DA rights only partially overlap. First, the DA rights, including their access component, do not seem to cover inferred data, while the GDPR right to access does.[64] Second, while the DA rights apply irrespective of the legal bases relied upon for justifying the initial processing, the GDPR introduces a conditional portability right, which is only triggered by two legal bases.[65] Third, the GDPR does not place any restrictions regarding to whom the personal data in scope for the right to portability can be ported to, while the DA, consistent with its objective of avoiding further data lock-in, prohibits gatekeepers from accessing data through data portability requests.[66]

As mentioned by the Hamburg DPA in its position paper on the DA, GDPR and DA rights should be conceived as cumulative rights,[67] which implies that the lex specialis argument, which may be leveraged to try to solve potential applicability matters, does not hold. Indeed, the domain and effects of a fundamental right are not necessarily the same as a market fairness prerogative. A cumulative application, however, raises questions about how supervisory authorities under the GDPR and competent authorities under the DA will collaborate in exercising their respective powers.[68]

6.2 The GDPR right to object

Article 21 GDPR grants data subjects the right to object to the processing of their personal data when it is based on public or legitimate interest grounds. This provision plays a central role in reinforcing individual control, particularly in contexts where consent is not the legal basis for processing.[69] In the evolving EU data governance landscape, sector-specific instruments have begun to supplement this general right.

The EHDS offers a notable example of rights-based data governance by introducing a layered opt-out regime to enhance individual control over personal electronic health data, which is a subcategory of electronic health data. For primary use, Member States may grant natural persons the right to opt out from the access to their

[64] Articles 4 and 5 DA only apply to readily available data, which is defined under Article 2(17) DA as data generated "without disproportionate effort going beyond a simple operation." Compare with Recital 63 GDPR, which mentions diagnoses, i.e., data points derived from the analysis of provided and observed data points. See also EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (2023) Version 2.1 para 97 <https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf>.accessed 17 June 2025. See also prior to the entry into applicability of the GDPR, Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994, [34-35]; AG Sharpston in joined cases C-141/12 and C-372/12 YS and others ECLI:EU:C:2014:2081 [44].

[65] Article 20(1)(a) GDPR.

[66] Articles 5(3) and 6(2)(d) DA. See also Bárbara Lazarotto, 'The right to data portability: A holistic analysis of GDPR, DMA and the Data Act' (2024) 15(1) European Journal of Law and Technology. The DA It also sets additional restrictions upon the types of processing a data recipient can perform. See Article 6 DA.

[67] HmbBfDI, 'Der Data Act Als Herausforderung Für Den Datenschutz' (2025) <https://datenschutz-hamburg.de/news/der-data-act-wie-lassen-sich-datenzugang-und-datenschutz-vereinbaren>.

[68] Tobias Baumgartner, Andreas Kellerhals and Sophie Tschalèr (eds), EuZ – Zeitschrift für Europarecht: Jahrbuch 2023 (buch & netz 2023).

[69] Assessing whether a right to object exists under Article 21 GDPR is not necessary to characterise the appropriate legal basis under Article 6 GDPR. Mousse [2025] CJEU C-394/23, ECLI:EU:C:2025:2 [70].

personal electronic health data registered in an electronic health record system through newly established electronic health data access services.[70] Most significantly, the EHDS directly grants an opt-out right for secondary use, allowing individuals to refuse the reuse of their personal electronic health data, e.g., for research, innovation, or health policy.[71] This right is designed to be easily exercisable and reversible.

Although both the GDPR and the EHDS rights aim to strengthen data subject autonomy, their interplay is not fully articulated. The GDPR's right to object sits within a horizontal legal framework, while the EHDS opt-out right emerges as a sectoral mechanism built for health data governance. The GDPR requires that objections be based on the data subject's specific situation, except in the case of direct marketing. In contrast, the EHDS opt-out right applies unconditionally, without requiring justification.[72] While this simplicity enhances accessibility for users, it also raises applicability questions: is the EHDS opt-out right a *lex specialis* implementation of GDPR rights, or does it constitute a cumulative sui generis mechanism with distinct legal status?

Rather than being in conflict, these rights should be understood as being cumulative and non-exclusionary prerogatives that operate in parallel to enhance individual agency at different levels.

This interpretative position should have important consequences from an implementation perspective. While the EHDS opt-out right is intended to be facilitated by the existence of a technical and interoperable infrastructure capable of consistently enforcing individual rights assertions across complex health data ecosystems,[73] nothing specific is introduced for the GDPR right to object. Yet, the GDPR right to object should still be relevant for data reuse that is performed on the basis of a task carried out in the public interest or in the exercise of official authority vested in the controller[74] or on the basis of a legitimate interest within the meaning of Article 6(1)(f) GDPR.[75] In other words, the GDPR right to object would be a right that operates at the project or permit level, as opposed to the infrastructure level, and would act as a safety valve in particular when the subsequent use is not carried out for scientific or historical research purposes or statistical purposes within the meaning of the GDPR. Given that personal data access for secondary use will happen in the context of secure processing environments, which could be operated by trusted data holders in several instances, the technological infrastructure could support a such a project-level right to object. From a technical standpoint, infrastructures capable of preserving data lineage are well-established and do not represent a major innovation.

[70] Article 10 EHDS.
[71] Article 71 EHDS.
[72] See Article 71(1) EHDS, which is however subject to exceptions set forth in Article 71(4) EHDS.
[73] See Article 75 EHDS.
[74] Unless personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) GDPR. See Article 21(6) GDPR.
[75] Article 21 GDPR read together with Article 6 GDPR.

7 Conclusion

This response to the CfE highlights the urgent need for coherence across post-GDPR regulations. Siloed approaches to core data governance concepts risk undermining both the credibility of future data strategies and the robustness of their foundational and horizontal layer—namely, the GDPR.

The terminology introduced in an attempt to build effective data governance structures, in part through regulation, is intricate and lack an overarching taxonomy. Post-GDPR regulations have not managed to build a consistent set of horizontal principles for data governance, which would be applicable to all data spaces, creating fragmentation and confusion. There is ambiguity surrounding the precise articulation of core concepts such as anonymisation and interplay between the different data access regimes. These challenges are problematic not only for legal certainty but also for the adequate protection of fundamental rights.

In light of these observations, this response aims to reaffirm that the GDPR remains the foundational layer of the EU's data governance architecture. This foundational role has direct implications for how newly introduced rights under sectoral and horizontal data laws should interact with existing GDPR rights.

In sum, this response underscores the need for a more integrated approach to regulatory interpretation and implementation, to be pursued in the near future through enhanced collaboration between competent authorities. This requires clearly expressing objectives, clarifying overlaps, and ensuring that sectoral innovations strengthen rather than weaken fundamental rights.