Privacy Next's Feedback on the Digital Omnibus Proposal

Key Points:

- **GDPR has expanded into a "law of everything," overextending its scope and weakening the data protection framework**
- **Supervisory authorities are overwhelmed by individual complaints, undermining enforcement, consistency, and public guidance on GDPR implementation.**
- **An overemphasis on individual data protection claims has sidelined the GDPR's equally important objective of enabling the free movement of personal data.**
- **A recalibration of GDPR priorities is needed to better balance fundamental rights, economic competitiveness, and administrative feasibility.**

Introduction

1. The European Commission's Digital Omnibus proposal comes at a time when the regional organisation and its Member States are pursuing a range of policy priorities - competitiveness, simplification, better enforcement, increased cooperation, and more efficiency are all identified as necessary matters to address. As with any reform process, the priorities being pursued are not always mutually compatible, and responses will also vary. In relation to the Digital Omnibus, concerns have been expressed regarding the diminution of the current governance frameworks for data protection, while at the same time, other views argue that innovation requires a limitation on the governance frameworks for data protection.

2. Privacy Next is of the view that these are not mutually exclusive choices in the process of legislative reform. The data governance framework has been built recognising the need to adapt to the technical and social developments in society while maintaining

sufficient safeguards for the protection of personal data. Both objectives must be pursued to ensure the effective functioning of the EU's Single/internal market.

3. The Draghi and Letta reports have made clear that the EU needs to reconsider the current regulatory systems and examine how to improve upon current approaches to regulation in order to support competitiveness, innovation, and the true realisation of the Single Market. The Digital Omnibus is only one part of the proposed wider reform process for the EU, but given the ways in which the data protection governance framework has evolved since the adoption of GDPR, particular attention is needed to the impact this regulation has had upon the ability of the EU to deliver on the benefits of the Single Market and upholding the fundamental rights of the Charter.

The GDPR as a Law of Everything

4. The transformation of the GDPR into a law of everything (Purtova, 2018; Lynskey, 2023) has created a system where an emphasis on breadth of application has overshadowed the creation of a complete and effective system for data protection. To protect the integrity of both the legal system and public administration, there must be a recalibration that distinguishes between actual violations of data protection on the one hand and effective administrative information management on the other. Without this, the GDPR will continue to be a burden on public and private resources while failing to provide meaningful protection for the rights that truly matter.

5. In its present form, the GDPR has contributed to an instrumentalisation of the law in a way that has weakened the framework. Complaints expressed as fundamental rights issues are very often tactical measures in the pursuit of other causes having nothing to do with data protection.

6. A recent case dismissed by the Austrian Federal Administrative Court (BVwG - W137 2328811-1) highlights how the elevation of GDPR rights leads to individuals abusing the system by making data protection claims in order to frustrate the ability of others to provide services. In this case, an individual who had a court order against them requiring

the payment of a debt made multiple GDPR claims when efforts were made to collect the debt. After the court order, the individual changed their address and name, moved to another Member State, and when the creditor contacted them to settle the debt, the individual made multiple claims that their fundamental rights to data protection had been violated. In the course of the proceedings, the debtor sent various claims and complaints to the creditor, the bar association of the creditor, the relevant supervisory authority, and the federal administrative court. All the time and effort spent by multiple bodies to reach a decision that an individual cannot use data protection claims to forego a legal judgment against them is a clear waste of resources.

7. The facts of this case are testament to how the GDPR has become a law of everything and how the system as a whole is suffering due to the ability of individuals to make anything and everything that is, in their view, a data protection complaint, thereby elevating the matter to a fundamental right. There are further examples where the GDPR is used in nefarious ways, such as a low-cost discovery tool in employment, family, or contract law, or where individuals challenge data handling processes instead of the substantive decisions in question.

8. The negative impact of the GDPR on economic activity and regulatory institutions has been documented in reports produced by the EU. The Second Report on the application of the General Data Protection Regulation (European Commission, COM(2024) 357 final) identified several matters concerning the application of GDPR having a negative impact across the system. These include –

- Diverging national interpretations of GDPR are leading to fragmentation across the Single Market.
- Economic actors, especially SMEs, are facing challenges in terms of resources and expertise to ensure compliance.
- National supervisory authorities are facing resource constraints affecting their ability to enforce and support compliance.

A range of other negative impacts was also identified, including consequences for international cooperation, limiting the EU's ability to lead on practical multilateralism cooperation.

9. A 2024 study by the EU Fundamental Rights Agency (*GDPR in practice – Experiences of data protection authorities*) emphasises that the demands of the GDPR have overwhelmed the ability of national supervisory authorities to fulfil their enforcement and compliance responsibilities. The study presents the burdens arising from the ongoing rise in complaints, data breach notifications, investigations, and cross-border cases since the adoption of GDPR, which has significantly increased the workload for supervisory authorities. This problem is most acute in relation to how the GDPR system has prioritised the management of individual complaints at the expense of authorities' ability to engage in public awareness activities or provide advice to organisations. The overall impact of GDPR on supervisory authorities creates delays and gaps in ensuring compliance, which, over time, further weaken the data protection system.

10. But GDPR has grown, and the understandings and interpretations put upon it have been highly selective in some situations, but certainly too ambitious. The difficulties start with the wording of GDPR in article 1(1), which sets the subject matter of the Regulation as “the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.” This second part, the free movement of personal data, has been relegated, and individual complaints regarding protection of personal data have been elevated beyond the two-purpose framing of GDPR. The matter is further complicated by article 1(2) GDPR, which claims that GDPR “protects fundamental rights and freedoms of natural persons”

11. As demonstrated in the recent EDPB/S joint opinion on the Digital Omnibus, such wording is used to cast the GDPR framework into a supra-constitutional instrument. The joint opinion, in its discussion on Data Subject Access Requests (DSARs), makes the claim that the article 1 provisions underline

> "that the GDPR, and more generally the right to protection of personal data in Article 8 of the Charter, aims to protect all individuals' fundamental rights and freedoms, and is not limited to the protection of personal data alone". (para. 54)

On a basic reading of this statement, it appears the EDPB/S is saying that GDPR and article 8 of the Charter are precursors to the protection of all fundamental rights and freedoms; that is to say, over and above the EU treaties and the constitutions of the Member States. This cannot be a correct interpretation of the EU's legal hierarchy, as the

GDPR is secondary legislation which is subject to revision over time and broader limitations than the foundational texts. But in the past eight years, the GDPR's provisions have been elevated far beyond other considerations of how the EU should work. In particular, the ways in which the GDPR gives individuals the right to contact any organisation about their data have created significant burdens upon the system and hindered the objectives of the Single Market.

Data Subjects Access Requests – When good intentions result in unmanageable complexity

12. While the GDPR is often perceived as working well due to high awareness both within the Single Market and globally, the system has come to the stage where processing and responding to the complaints of individuals has taken priority, regardless of the negative consequences for the efficiency and integrity of the system. As with the example from the Austrian Federal Administrative Court above, it is necessary to recognise that while the ability of data subjects to control their data is fundamental to an effective data protection governance system (article 8, Charter), the GDPR has also empowered individuals to make demands that have little to do with data protection and are better described as an abuse of the system.

13. The current state of play surrounding DSARs shows how GDPR has resulted in an unworkable system, as individuals have been given unfettered access rights to make data protection claims in any and almost all circumstance. Even if there is no evidence of their

data being processed, individuals can still contact companies to check. The right of access to personal data is foundational, and a key to transparency, but it remains unclear how a system allowing for selfish exploitation is able to effectively uphold the data protection rights of all, much less support the effective functioning of the Single Market. From an enforcement perspective, creating a system of private-individual enforcers, by allowing every natural person in the EU to monitor and file complaints against any company that may be processing their personal data, does not appear to be delivering effective results for the data protection system as a whole.

14. The current *Brillen Rottler* case before the CJEU (C-526/24, (decision due 19 March 2026) illustrates the challenges DSARs pose to the data protection system due to individual self-interest. In this case, an individual voluntarily signed up to an online newsletter, willingly sharing their personal data with that company. Within two weeks, the individual made a DSAR to the company. The company rejected the request, saying it was abusive. The individual immediately escalated the matter, claiming compensation, petitioning the relevant supervisory authority and then the case went to the national courts and is now before the EU court. The company's reasons to deny the request should have been valid on the most common-sense level, as there can be no objective reason for any individual to have immediate data protection concerns over a simple voluntary transaction. Notably, there is a public record of this individual making similar requests to other companies and subsequently seeking compensation when the individual deems the responses unsatisfactory.

15. The Advocate-General's opinion in the case suggests that limitations on DSARs should be minimal, placing a high burden on data controllers to prove that a request is abusive or excessive. While acknowledging that some DSARs may be vexatious, the Advocate-General indicates that merely submitting multiple requests is insufficient to demonstrate abuse. Furthermore, the Advocate-General stated that using publicly available information about the behaviour of the data subject cannot be used as a factor in arriving at a decision about the DSAR. What the Advocate-General does not explain is why such behaviour should be allowed on an unquestioned basis under the claim of a

fundamental right, when its result is a disruption to the activities of economic actors and public authorities, and the actions being litigated are far removed from data protection.

16. The question raised by this example is not the right of individuals to access their data. Rather, the question is about how the right has come to be exercised by individuals under GDPR, which has expanded the content and institutional reach of the right to almost unreasonable parameters. The expansion is clear in article 15(1) GDPR, whereby any individual in the EU can contact any organisation to ask whether their data is being processed. From this, the GDPR empowers individuals to request extensive information about their data and how it has been processed. Furthermore, article 12 GDPR sets out a range of obligations on data controllers when responding to DSARs, which must be done within one month, requiring a company to allocate significant resources to a situation that is not about economic activity or even upholding fundamental rights.

17. In the EDPB's current guidance on DSARs (Guidelines 1/2022), they appear to support an unlimited self-interested approach by stating that an access request cannot be deemed excessive even if no reasons for the request are given, if the data subject uses improper language, or if the data subject intends to file further claims (para. 109). These parameters are an invitation to overburden the system and make lack of civility by complainants, even rudeness, a part of fundamental rights. In the joint response to the Digital Omnibus, the EDPB/S seeks to disassociate the notion of "abuse of rights" from the right of access for reasons other than data protection. This reasoning is consistent with the joint opinion's placement of GDPR and Article 8 over and above all other constitutional values in the EU system, but it is unrealistic and unworkable, especially for national supervisory authorities that lack the necessary resources to handle the scale of individual complaints being faced.

Creating a system of effective data protection in the Single Market

18. The current implementation of GDPR has imposed significant burdens that hinder the competitiveness of businesses, particularly SMEs. There has also been substantial

strain on national supervisory authorities, which lack the resources to handle all complaints, leaving them unable to carry out other activities that would support an effective data protection framework. The current system has also led to fragmentation due to divergent national interpretations, adding to an already complex regulatory environment and further hindering innovation and economic activity.

19. Above, we have pointed out how current interpretations of GDPR have resulted in many negative results. We are not calling for an end to GDPR, only a recalibration of the priorities within the system. In this regard, it is essential to note that GDPR is not just about the protection of personal data. In the article 1(1) subject matter, the regulation also addresses "rules relating to the free movement of personal data." This is reinforced by article 1(3) whereby the free movement of personal data cannot be restricted or prohibited "for reasons connected with the protection of natural persons with regard to the processing of personal data." But somehow, this part of GDPR has not had the same level of respect or attention.

20. Throughout the GDPR recitals, the importance of the free flow of data is set out as a fundamental component of the overall Single Market system. For example, Recital 2 explains how the regulation is to contribute to the EU's area of freedom, security and justice, as well as "an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market", all of which contribute to the "well-being of natural persons." Recital 5 recognises that the growth of the Single Market has led to a substantial increase in cross-border data flows. And Recital 9 explains how, in this context, the previous Directive 95/46/EC had not been able to remove barriers to the free flow of data, constituting an obstacle to economic activities across the Single Market. Recital 13 makes clear that the functioning of the internal market requires the free movement of personal data.

21. All these references recognise that the free flow of data must also ensure data protection for natural persons, but this protection is not the primary or absolute objective of the data protection framework. In fact, it must be re-emphasised that the GDPR itself explains that the right to the protection of personal data is not an absolute right; it must

be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. (Recital 4)

22. Further studies need to be done as to how the more absolutist approach to data protection has come to be so preeminent in the EU and the impact such an approach has had, both positive and negative. But as Draghi and Letta make clear, something must change. The fragmentation of the Single Market, whereby there are different approaches and standards to data protection, is not beneficial for anyone. The excessive burdens being put on economic actors, and by extension, supervisory authorities and the courts, are preventing the further development of an effective data protection system.

23. It is important to keep in mind that article 57 GDPR places twenty-two different tasks under the responsibility of supervisory authorities. These tasks range from public awareness-raising, advising parliaments, general monitoring, supporting credit systems and bodies, supporting data controllers' awareness, and cross-border cooperation. Of the twenty-two listed tasks in article 57, only two directly relate to the right of data subjects to complain, yet those two tasks dominate the time and resources of most authorities. Questions therefore need to be asked about a system that has reached this stage of uneven development, because a rights framework that is impossible to administer at scale is a rights framework that fails to deliver in practice.

Going forward with the Legislative Process

24. The Commission GDPR proposals in the Digital Omnibus continue to raise significant concerns and questions. There is no doubt that in the eight years the regulation has been in force, the protection of personal data has evolved considerably. At the same time, the practical realities of the governance framework created by GDPR are under significant stress with respect to operability, effectiveness, and consistency. The current reform process is an opportunity to recalibrate the system that has evolved from the GDPR in order to ensure the fundamental right to data protection, as set out in Article 8 of the Charter of Fundamental Rights in the EU, is realised. The overly complex approach

created by GDPR is not the answer, and neither is viewing data protection as an almost absolute right which is not to be questioned in any way.

25. The debates and discussions about how best to ensure the protection of personal data do not start and end with GDPR. The Digital Omnibus is only a first step, a proposal from the Commission that is being examined by the EU co-legislators (the Council and Parliament). Whether or not proposed reforms are accepted or rejected at this stage does not end the examination of how best to ensure data protection. The GDPR recognises the changing nature of technology and the needs of society, requiring flexibility and adaptation. Too many voices in the current debate are calling for no changes whatsoever, but democracy is built on regular debate and discussion about the nature of laws to meet society's needs. The current proposal provides an opportunity for such engagement, which we welcome.

Privacy Next is of the view that, in shaping the next generation of privacy, it is imperative to recognise that technology, and the ways in which personal data is processed, present benefits to society that should be supported. Current interpretations of GDPR do not always account for the range of interests involved in data protection. For the continued growth and development of the Single Market as a beneficial part of our societies, the views of all stakeholders, and not just particular sections of society, are relevant. We hope the broader processes surrounding future debates about the Digital Omnibus provide opportunities for new ideas to be considered and existing frameworks to be questioned.

Submitted 15 March 2026