REDEFINING 'PERSONAL DATA' IN THE DIGITAL OMNIBUS PROPOSAL: IMPLICATIONS FOR AI PROCESSING BY EU INSTITUTIONS UNDER REGULATION (EU) 2018/1725

Emilian MATEICIUC [(*)]

Abstract

Published on 19 November 2025, COM(2025) 837 final proposes amendments to both the GDPR and Regulation (EU) 2018/1725 within the broader Digital Omnibus simplification package. This paper examines one of the proposal's most consequential moves, namely the attempt to codify a relative, entity-specific approach to identifiability within the definition of personal data. Its central claim is that the proposed alignment between the GDPR and the EUDPR cannot be assessed only as a drafting exercise. Once projected onto the institutional framework of the Union, the amendment raises specific questions that the proposal does not sufficiently address, especially in relation to the supervisory role of the European Data Protection Supervisor, inter-institutional data environments, and AI-related processing involving pseudonymised and potentially sensitive datasets. Methodologically, the paper combines doctrinal analysis of the proposed legislative text with close reading of the Court of Justice's judgment in EDPS v Single Resolution Board, the earlier line of case law from Breyer and OC v Commission, and Joint Opinion 2/2026 of the EDPB and EDPS. The article argues that the proposal appears to move beyond clarification and risks materially reshaping the scope of EU data protection law in the institutional context. It concludes that legislative parallelism between the GDPR and the EUDPR remains desirable, but only if accompanied by safeguards tailored to EU institutions.

Keywords*: Digital Omnibus, personal data, EUDPR, EU institutions, artificial intelligence.*

1. Introduction

The European Commission's Digital Omnibus proposal of 19 November 2025 presents itself as a simplification measure within the Union's digital legislative framework. Yet, in the field of data protection, simplification is not merely a technical exercise. Where amendments concern the scope of 'personal data', the threshold of identifiability, and AI-related derogations, their effects extend beyond compliance costs and directly affect the level of protection granted under Union law. This is particularly true in relation to Regulation (EU) 2018/1725, which governs the processing of personal data by Union institutions, bodies, offices and agencies.

This article examines whether the proposed alignment between the GDPR and the EUDPR remains normatively coherent once applied to AI-related processing by EU institutions. Its core claim is that the proposal assumes a degree of parallelism between the two regimes that is not fully justified. Legislative alignment may appear desirable at the level of drafting technique. But the institutional environment of Union bodies, the supervisory role of the EDPS, and the public-law functions performed by EU institutions generate legal effects that are not reducible to the GDPR model.

[(*)] PhD Candidate, Faculty of Law, "Nicolae Titulescu" University, Bucharest (e-mail: e.mateiciuc@mailfence.com).

The issue has acquired particular significance after the Court of Justice's judgment in EDPS v SRB and after the EDPB-EDPS Joint Opinion 2/2026 on the Digital Omnibus proposal. Taken together, these developments show that the concept of personal data cannot be treated as a static or purely abstract category. Its application depends on context, on the position of the recipient, and on the legal environment in which data are processed.

The discussion begins with the proposed amendments to the GDPR-EUDPR relationship and the case law that has shaped the concept of identifiability. It then examines the implications of EDPS v SRB for the interpretation of 'personal data' in institution-specific AI deployments. Next, it explains why AI-related processing by EU institutions cannot be treated as a simple extension of private-sector GDPR compliance. It finally proposes a more differentiated approach to legislative alignment, one that preserves coherence without obscuring the specific legal position of EU institutions.

2. The concept of personal data under EU law: from Breyer to EDPS v SRB

The definition of personal data sits at the foundation of the EU data protection framework. Article 4(1) of Regulation (EU) 2016/679 (GDPR) defines personal data as any information relating to an identified or identifiable natural person, where identifiability is assessed by reference to all means reasonably likely to be used by the controller or by another person.[1] Article 3(1) of Regulation (EU) 2018/1725 (EUDPR) contains an almost identical provision, applicable to Union institutions, bodies, offices and agencies.[2] The co-legislators sought to maintain broad substantive alignment between the GDPR and the EUDPR, while preserving the institutional specificity of the latter.[3]

The scope of this definition has never been self-evident. Recital 26 of the GDPR clarifies that the assessment of whether means are reasonably likely to be used for identification should take into account all objective factors, including cost, time, and available technology.[4] Yet the recital leaves open a question that has divided both courts and commentators: must identifiability be assessed from the perspective of the specific controller processing the data, or in the abstract, taking into account any party that might conceivably achieve identification?

The Court of Justice addressed this tension for the first time in Breyer v Bundesrepublik Deutschland. The case concerned dynamic IP addresses stored by a website operator who did not, by itself, hold the information needed to link those addresses to natural persons. The internet service provider did. The Court held that data qualifies as personal where the controller has legal means available to obtain additional information enabling identification. The test was not whether identification was theoretically possible, but whether the

[1] 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, art. 4(1).

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, art. 3(1).

[3] See recital 5 of Regulation (EU) 2018/1725, which states that the rules on data protection applicable to Union institutions should be aligned with the approach taken in Regulation (EU) 2016/679.

[4] Regulation (EU) 2016/679, recital 26.

controller had access to means reasonably likely to be used.[5] This formulation already pointed towards a relative reading of identifiability, though the Court did not frame its reasoning in those explicit terms.

In OC v European Commission, the Court further developed the case-law on identifiability under the EUDPR. The case concerned codes assigned to individuals who had participated in a selection procedure. The judgment sharpened the Breyer reasoning by placing greater emphasis on the controller-specific assessment: what matters is not some abstract capacity to identify, but whether the particular entity processing the data possesses or can obtain the means to do so.[6]

The most significant development came with EDPS v Single Resolution Board, decided on 4 September 2025. The Single Resolution Board had collected comments from stakeholders during a public consultation, replaced respondents' names with alphanumeric codes, and transmitted the coded responses to a consultancy firm for analysis. The EDPS took the position that the transmitted data remained personal data, since the SRB itself retained the identification key. The Court of Justice, sitting as First Chamber, disagreed in part. It confirmed that pseudonymised data does not automatically constitute personal data in the hands of every recipient. For the recipient, the decisive issue was whether it had, or could reasonably obtain, the means enabling re-identification.[7]

Two aspects of the judgment deserve particular attention in the present context. First, the case arose under the EUDPR, not the GDPR. The SRB is an EU agency. The Court nonetheless confirmed a uniform approach to interpretation, given the parallel definitions used in both instruments. This matters because it means that the institutional data protection framework is not merely a passive mirror of the GDPR; it actively generates case law that shapes the interpretation of the concept of personal data across the wider EU legal order.[8]

Second, the judgment treats identifiability as a relational property, not an intrinsic attribute of the data. The same dataset can be personal data for one controller and non-personal for another. This position has practical consequences that go well beyond the facts of the SRB case. In any environment where multiple institutions share, transfer, or jointly process pseudonymised datasets, the legal qualification of the data becomes dependent on who is processing it and what means that entity has at its disposal. The implications for inter-institutional data flows and for the deployment of AI systems trained on pseudonymised datasets are immediate, and they form the subject of the analysis that follows.

The Breyer-to-SRB line of case law did not emerge in a vacuum. It reflects a broader tension between two competing visions of data protection. One vision, protective and expansive, treats any theoretical possibility of identification as sufficient to trigger the full apparatus of data protection law. The other, pragmatic and contextual, insists that legal obligations should attach only where identification is a realistic prospect for the specific entity concerned. The Digital

[5] Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779, judgment of 19 October 2016, paras 42-49.

[6] Case C-479/22 P, OC v European Commission, ECLI:EU:C:2024:215, judgment of 7 March 2024.

[7] Case C-413/23 P, European Data Protection Supervisor v Single Resolution Board, ECLI:EU:C:2025:645, judgment of 4 September 2025.

[8] Court of Justice of the European Union, Press Release No 107/25, "The Court of Justice clarifies the scope of the concept of personal data in the context of a transfer of pseudonymised data to third parties", 4 September 2025.

Omnibus proposal appears to move in that direction, but whether it merely clarifies or materially reshapes the legal concept remains contested.

3. The Digital Omnibus proposal: codification, clarification, or redefinition?

On 19 November 2025, the European Commission published a proposal for a Regulation amending, among other instruments, Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.[9] The stated objective is simplification: reducing compliance friction and making the EU digital legal framework more accessible.[10] Among the proposed amendments, the modification of the definition of personal data in Article 4(1) GDPR has attracted the most attention and the sharpest criticism.

The Commission proposes to add a new paragraph to Article 4(1), specifying that identifiability must be assessed from the perspective of the controller or processor, taking into account the means reasonably likely to be used by that specific entity for identification purposes.[11] The proposal frames this as a codification of the approach confirmed by the Court of Justice in EDPS v SRB, not as a change in substance. The Explanatory Memorandum presents the amendment as a clarification intended to bring legal certainty and to reflect the current state of the case law.[12]

This framing is contested. In Joint Opinion 2/2026, adopted on 10 February 2026, the EDPB and the EDPS acknowledge the objective of legal clarity but argue that inserting an entity-specific identifiability test into the operative text of the Regulation goes beyond mere clarification and risks narrowing the material scope of data protection.[13] They recommend that the co-legislators refrain from amending the definition in the operative provisions and, if clarification is deemed necessary, confine it to a recital.[14]

The distinction between operative text and recital is not formalistic. A recital provides interpretive guidance; it does not create autonomous legal obligations. An entity-specific identifiability criterion placed in a recital would serve as an aid to interpretation, pointing courts and supervisory authorities towards the contextual approach without displacing the existing definition. The same criterion placed in the operative text becomes a binding rule that controllers can invoke directly, potentially shielding certain categories of processing from the application of data protection law where the controller argues that it lacks the means for identification. The difference between these two legislative techniques is not trivial. It determines whether the contextual approach functions as one factor in a broader assessment or as a standalone threshold that gates the applicability of the Regulation.[15]

The proposal does not confine its amendments to the GDPR. COM(2025) 837 also amends Regulation (EU) 2018/1725

[9] European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557, COM(2025) 837 final, 19 November 2025.

[10] *Ibid.*, Explanatory Memorandum, Section 1.

[11] *Ibid.*, article 3, point (1), amending article 4(1) of Regulation (EU) 2016/679.

[12] *Ibid.*, Explanatory Memorandum, Section 5, sub-section on the definition of personal data.

[13] European Data Protection Board and European Data Protection Supervisor, Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework, adopted on 10 February 2026, para. 13.

[14] *Ibid.*, paras 14-21.

[15] *Ibid.*, paras 20-21.

with corresponding provisions.[16] Joint Opinion 2/2026 notes that the observations made in respect of the GDPR amendments also apply to the corresponding proposals for amendments to the EUDPR, while identifying specific cases where full alignment between the texts does not function adequately.[17] This acknowledgement is significant: it confirms that the Commission has, in essence, applied the same legislative technique to both instruments, transposing GDPR-oriented amendments into the EUDPR without a separate assessment of whether they suit the institutional context.[18]

The approach is not unprecedented. The EUDPR was itself drafted as a parallel instrument to the GDPR, and the co-legislators deliberately aligned most of its substantive provisions with the GDPR text.[19] But alignment as a drafting method has limits. The GDPR governs a vast and heterogeneous array of private and public controllers across twenty-seven Member States. The EUDPR governs a comparatively small number of Union institutions, bodies, offices and agencies, each operating within a distinct administrative and legal environment, subject to the supervision of a single authority, the EDPS. The question is whether an amendment designed primarily to address private-sector compliance concerns, and motivated in part by the desire to create regulatory space for AI development, is equally suited to the institutional framework in which the EUDPR operates.

The Digital Omnibus package also interacts with separate proposals relevant to the processing of special categories of data in the context of AI. The AI Act already contains a derogation permitting the processing of sensitive personal data for the purpose of detecting and correcting bias in AI systems classified as high-risk.[20] The companion AI Omnibus proposal would extend that derogation beyond the current high-risk perimeter. In Joint Opinion 1/2026, the EDPB and the EDPS expressed concern that expanding the derogation without maintaining strict necessity requirements could undermine the protection afforded to sensitive data.[21] That concern acquires specific weight in the EUDPR setting, where institutional data environments may involve large, interoperable and difficult-to-contest datasets.

The next section examines these consequences in greater detail, focusing on the structural features of institutional data processing that distinguish it from the private-sector context for which the Digital Omnibus was primarily conceived.

4. Implications for AI-related processing by EU institutions

The preceding sections have established that the Digital Omnibus proposal codifies a relative approach to identifiability and transposes it into the EUDPR through mirror amendments contained in Article 4 of COM(2025) 837. The EDPB and the EDPS have accepted the principle of alignment but have flagged

[16] COM(2025) 837 final, article 4, amending Regulation (EU) 2018/1725.
[17] Joint Opinion 2/2026, para. 13.
[18] *Ibid*., para. 21.
[19] Recital 5 of Regulation (EU) 2018/1725.
[20] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 12.7.2024, art. 10(5).
[21] European Data Protection Board and European Data Protection Supervisor, Joint Opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence, adopted on 20 January 2026, paras 8-16, especially 11-13.

specific cases where it does not work.[22] This section examines why those cases matter most precisely where they have received the least attention: in the institutional data environments of the Union.

EU institutions do not process data the way a private company does. The differences are structural, not merely quantitative. Union bodies operate within a framework of public-law obligations, shared databases, and inter-institutional cooperation arrangements that have no equivalent in the private sector. Their supervisory authority is singular (the EDPS) rather than distributed among twenty-seven national authorities. And their data processing activities increasingly involve AI systems that operate across institutional boundaries.

The most instructive example is eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. eu-LISA operates, among others, the Schengen Information System (SIS II), the Visa Information System (VIS), Eurodac, and the Entry/Exit System (EES).[23] These are not isolated databases. Following the adoption of the Interoperability Regulations in 2019, they are designed to be interconnected through shared components, including a common identity repository (CIR), a multiple-identity detector (MID), and a European search portal (ESP).[24] The interoperability architecture is built on the assumption that data from one system can be cross-referenced against data from another. The common identity repository, in particular, enables cross-system queries that can link records across databases which, taken individually, contain only pseudonymised data. In such an environment, the question of whether a given entity has the means to identify a data subject is not a binary one. It depends on the level of access granted to that entity within the interoperability framework, and that access can change depending on the operational context.

This is where the proposed entity-specific identifiability standard creates a problem that the GDPR context does not face with the same intensity. Under the current framework, if an EU institution processes pseudonymised data and does not itself hold the re-identification key, it can argue, following the logic of EDPS v SRB, that the data is not personal data for it. But the interoperability architecture means that re-identification capacity is not fixed. An agency that cannot identify a data subject today may gain that capacity tomorrow through a lawful query to the common identity repository. The proposed amendment does not address this temporal dimension. It freezes the assessment of identifiability at the moment of processing, without accounting for the shifting access

[22] EDPB-EDPS Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework, adopted on 10 February 2026, para. 10, in fine, read together with para. 13.

[23] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), OJ L 295, 21.11.2018.

[24] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa, OJ L 135, 22.5.2019, arts 17 (European search portal), 17a (common identity repository) and 25 (multiple-identity detector); Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, OJ L 135, 22.5.2019, arts 13, 13a and 21 (corresponding provisions).

structures that characterise inter-institutional data environments.[25]

The EDPB and the EDPS have signalled a related concern in Joint Opinion 2/2026. They warn that the proposed changes could induce controllers to seek loopholes, including by artificially outsourcing activities or capabilities to separate entities in order to remove processing from the scope of data protection law.[26] In the private sector, such structuring requires deliberate effort. In the institutional context, the separation already exists by design: different agencies, different mandates, different access levels within the same interoperability framework. The risk is not that EU institutions will game the system, but that the system itself, once the entity-specific standard is codified, will produce results that are technically correct but functionally inadequate.

The supervisory dimension reinforces the concern. The EDPS supervises all Union institutions and bodies under the EUDPR. If the entity-specific approach narrows the category of data that qualifies as personal in the hands of a particular institution, the EDPS may find its supervisory jurisdiction reduced, not because of a policy choice, but as a side effect of a definitional change designed for a different regulatory context. Joint Opinion 2/2026 itself, in the context of DPIA lists, states that the Commission should not be given the possibility of shaping the extent of its own obligations under the EUDPR. That reasoning, although formulated in a different context, points, in our view, to a broader principle: changes that indirectly affect the scope of EDPS oversight require distinct institutional justification, not automatic transposition from the GDPR.[27]

The interaction with AI-related derogations adds a further layer. The current AI Act permits the processing of special categories of personal data for the purpose of detecting and correcting bias in high-risk AI systems, subject to strict necessity.[28] The companion AI Omnibus proposal would introduce a new Article 4a extending this derogation to providers and deployers of all AI systems and models.[29] The EDPB and the EDPS have recommended that the standard of strict necessity be maintained and that the scope of the derogation be clearly circumscribed to cases where bias is likely to affect health, safety, or fundamental rights.[30]

For EU institutions, this extension matters in a specific way. Institutional AI deployments (document management, HR screening, translation workflows, risk assessment) often involve datasets that contain residual sensitive information. The EUDPR applies the same prohibition on processing special categories of data as the GDPR, based on Article 10 EUDPR and the corresponding derogations. If the bias detection derogation is extended to all AI

[25] The author's own assessment, building on the reasoning in Case C-413/23 P, EDPS v SRB, ECLI:EU:C:2025:645, paras 84-85, and the structural features of the interoperability framework established by Regulations (EU) 2019/817 and 2019/818.

[26] Joint Opinion 2/2026, para. 17. The EDPB and EDPS note the risk that controllers could implement nominal measures to separate their processing activities from the means reasonably likely to be used to identify the data subjects, seeking to remove them from the scope of the GDPR/EUDPR. See also fn 25 of the Joint Opinion.

[27] Joint Opinion 2/2026, para. 91, in the context of the proposed amendments to DPIA lists under Article 39 EUDPR. See also para. 107, where the EDPB and the EDPS note that proposed Article 88a GDPR and proposed Article 37 EUDPR cannot be implemented and enforced without the provision of supervisory powers, and call for the inclusion of fining powers for the EDPS under Article 66(3) EUDPR.

[28] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024, Article 10(5).

[29] EDPB-EDPS Joint Opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence, adopted on 20 January 2026, para. 8.

[30] Joint Opinion 1/2026, paras 11-13.

systems, and the definition of personal data is simultaneously narrowed, institutions could find themselves in a regulatory grey zone: processing data that may or may not qualify as personal, under a derogation that may or may not apply, with supervision by an authority whose jurisdiction depends on the answer to the first question. The result is not simplification but the creation of legal uncertainty at the precise point where clarity is most needed.

Joint Opinion 1/2026 underscores that DPAs remain competent to supervise the processing of personal data under the new Article 4a, including in the institutional context where the EDPS fulfils that role.[31] But this competence presupposes that the data in question qualifies as personal. If the proposed definitional change removes certain categories of pseudonymised data from the scope of the EUDPR, the supervisory competence of the EDPS over those categories of processing would be removed with it, regardless of the intentions of the co-legislators.

The concern is not confined to administrative processing. The EUDPR also contains a dedicated operational layer in Chapter 9, aligned with the Law Enforcement Directive, and the Commission has identified the need for a targeted amendment of that chapter.[32] If the definitional changes introduced by the Digital Omnibus enter into force before that amendment is finalised, the institutional framework risks being reshaped in stages, without a coherent view of how the pieces fit together. The problem is not hostility to institutional data protection, but the absence of a distinct institutional calibration in the proposal. The explanatory memorandum focuses on compliance burdens for private operators and SMEs. The EDPB and the EDPS observed that the proposal was not accompanied by a full impact assessment[33]. The proposal contains no separate assessment of how the amendments would affect data processing by Union institutions under the EUDPR. The result is a set of amendments that may function adequately in the GDPR setting while producing unintended consequences in the institutional one.

5. Conclusions

This article has examined the implications of the Digital Omnibus proposal for AI-related data processing by EU institutions under Regulation (EU) 2018/1725. Its core finding is that the proposed amendments, while defensible in the GDPR context for which they were primarily designed, do not adequately account for the structural features of the institutional data protection framework.

Three points follow from this analysis.

First, the codification of entity-specific identifiability in the definition of personal data is not a neutral clarification. As the EDPB and the EDPS have argued, it goes beyond the targeted codification of CJEU jurisprudence and risks narrowing the material scope of both the GDPR and the EUDPR. In the institutional setting, the problem is compounded by the interoperability of large-scale IT systems and by the fluid nature of inter-institutional data

[31] Joint Opinion 1/2026, para. 16.

[32] The EUDPR contains a dedicated chapter (Chapter 9) for operational processing aligned with Directive (EU) 2016/680. The need for a targeted amendment was identified in the Commission's report on the application of the EUDPR: European Commission, Report on the first two years of application of Regulation (EU) 2018/1725, COM(2022) 530 final, 14 September 2022, section 5.2, proposing to clarify that the EUDPR entrusts the EDPS with the supervision of the law enforcement chapter and with the powers granted to it under Article 58 EUDPR.

[33] Joint Opinion 2/2026, para. 7.

access. The proposed amendment does not account for the possibility that identification capacity may shift depending on operational context, and it offers no mechanism to address the resulting regulatory uncertainty.

Second, the approach of mirror amendments, transposing GDPR-oriented provisions into the EUDPR without separate assessment, reaches its limits precisely where the institutional context diverges from the private-sector one. The EUDPR was designed as a parallel instrument, but parallelism as a legislative technique does not eliminate the need for context-specific evaluation. The EDPB and the EDPS have themselves acknowledged that full alignment is not always appropriate. This article has identified specific cases (interoperability, EDPS supervisory scope, AI-related derogations for special categories of data) where the absence of such evaluation risks producing unintended consequences.

Third, the extension of the bias detection derogation to all AI systems and models, combined with the narrowing of the personal data definition, creates a regulatory grey zone for institutional AI deployments. The strict necessity standard recommended by the EDPB and the EDPS would offer a partial safeguard, but only if the data in question remains within the scope of the EUDPR in the first place. The two amendments interact in ways that the proposal does not address.

The expected impact of these findings is primarily directed at the legislative process. As the proposal progresses through the European Parliament and the Council, the institutional dimension of the EUDPR amendments deserves separate scrutiny, not as an afterthought to the GDPR debate but as a distinct question with its own legal and operational parameters. The EDPS, as the authority responsible for supervising data processing by Union institutions, is well placed to contribute to this assessment, and the forthcoming EDPB guidelines on pseudonymisation and anonymisation may provide additional analytical tools.

Further research should extend the analysis in two directions. The first concerns the operational dimension: a detailed examination of how the proposed amendments would affect specific institutional data flows, including those managed by eu-LISA and the European Commission's internal AI deployments. The second concerns the forthcoming targeted amendment of Chapter 9 of the EUDPR, which governs operational and law enforcement-style processing by Union institutions. The interaction between the Digital Omnibus amendments and that parallel legislative process has not yet been examined in the literature and may raise additional questions about the coherence of the institutional data protection framework.

References

- Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4.5.2016.
- Regulation (EU) 2018/1725, OJ L 295, 21.11.2018.
- Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L, 12.7.2024.
- European Commission, Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557, COM(2025) 837 final, 19 November 2025.
- European Data Protection Board and European Data Protection Supervisor, Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework, adopted on 10 February 2026.

- European Data Protection Board and European Data Protection Supervisor, Joint Opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence, adopted on 20 January 2026.
- Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779, judgment of 19 October 2016.
- Case C-479/22 P, OC v European Commission, ECLI:EU:C:2024:215, judgment of 7 March 2024.
- Case C-413/23 P, European Data Protection Supervisor v Single Resolution Board, ECLI:EU:C:2025:645, judgment of 4 September 2025.
- Court of Justice of the European Union, Press Release No 107/25, "The Court of Justice clarifies the scope of the concept of personal data in the context of a transfer of pseudonymised data to third parties", 4 September 2025.
- European Commission, Report on the first two years of application of Regulation (EU) 2018/1725, COM(2022) 530 final, 14 September 2022.
- Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), OJ L 295, 21.11.2018.
- Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa, OJ L 135, 22.5.2019.
- Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, OJ L 135, 22.5.2019.