European Law Blog

“Personal Data”: More Than a Definition, a Quasi-Constitutional Stake in EU Law in the Era of the Digital Omnibus

Pablo Trigo Kramcsák Barbara Lazarotto

European Law Blog

Published on: Mar 02, 2026

URL: https://www.europeanlawblog.eu/pub/yc0l0slk

License: Creative Commons Attribution-ShareAlike 4.0 International License (CC-BY-SA 4.0)

The definition of "personal data" appears, at first glance, to be a technical provision: one among many definitional clauses. In EU law, however, it performs a far more consequential role. It determines the material reach of Article 8 of the Charter of Fundamental Rights (CFR) and Article 16 of the Treaty on the Functioning of the European Union (TFEU), structuring the operation of the Union's digital rights framework. For this reason, any amendment to the definition (even if presented as merely clarificatory or procedural) carries constitutional significance.

This post argues that the notion of personal data has acquired a quasi-constitutional status within the EU legal order. It is not just a regulatory term in secondary legislation, but the legal gateway through which a fundamental right becomes operational. Modifying it is therefore not an ordinary legislative refinement, but a constitutional intervention.

Recent discussions about revising some elements of the definition, including within the Commission's Digital Omnibus initiative, bring this issue into focus. Yet the constitutional question precedes any specific proposal. To grasp what is at stake, we must first understand what the definition of personal data has come to represent.

From Regulatory Concept to Constitutional Gateway

The right to data protection was not established primarily at the EU level as a constitutional right. Early national data protection laws in the 1970s and the Council of Europe's Convention 108 laid important groundwork for the 1995 Data Protection Directive (DPD), which provided the first comprehensive EU framework and adopted a deliberately broad definition of personal data in Article 2(a): "any information relating to an identified or identifiable natural person."

However, the turning point in the definition came in 2000. Article 8 CFR recognised the right to the protection of personal data as an autonomous fundamental right, distinct from Article 7's right to private life. Though its wording is not explicit, Article 8 CFR's normative basis emerges from Court of Justice of the European Union (CJEU) case law and subsequent legislation, which show it protects individual control over personal data, making the concept of personal data central to this fundamental right.

The right is further shaped by the extensive EU data protection acquis, which has rendered data protection one of the most regulated fundamental rights in the EU, achieving a degree of autonomous scope rarely matched by other rights. In this connection, it draws its content from secondary legislation. The link between Article 8 and prior legislation is particularly evident in how it frames 'personal data.' Rather than providing an independent definition, it presupposes the concept as developed in existing legislation. In this way, the Charter's protection reflects and reinforces principles already articulated in secondary law. The notion of "personal data" under Article 8 therefore aligns broadly with the definition established by the DPD (in Article 2(a)) and international instruments.

The echoes from mutual influence between primary and secondary law do not stop there. The requirement outlined in Article 8(3) of the CFR regarding control by independent authorities was influenced by the Law Enforcement Directive, later incorporated into the GDPR. The same can be said regarding the principles of fairness, lawfulness, and purpose limitation, as well as the right to data access and rectification.

Initially, the Charter's provisions served as interpretive guidance. The Treaty of Lisbon, enacted in 2009, elevated them to primary law, granting the CFR binding effect equivalent to that of the Treaties. Constitutionalising the fundamental right to data protection through Article 8 CFR and Article 16 TFEU, which provided the legal foundation for the GDPR, enabling the Union to move beyond the DPD's minimum-harmonisation model.

When the GDPR was enacted, it largely retained the DPD's definition of personal data. Article 4(1) GDPR preserves the core formula ("any information relating to an identified or identifiable natural person") while clarifying certain elements in light of technological developments, including online identifiers and location data, which had already been encompassed in practice and affirmed by the CJEU in cases such as *Google Spain* (C-131/12) and *Breyer* (C-582/14). In doing so, the GDPR formalised and made explicit what had previously been implicit in the DPD, consolidating a broad and adaptable definition capable of addressing evolving technological contexts.

Although the GDPR is secondary legislation under Article 288 TFEU, its close connection to Article 8 CFR and Article 16 TFEU gives the definition of personal data a constitutional role. It serves as both the cornerstone of the scope of the fundamental right to data protection and as an interpretive reference for later legislation, even when such acts are at the same level of secondary law. In this way, the definition of personal data holds a structurally unique position. It determines the scope of a constitutional right. Without "personal data," Article 8 has no object. The definition is not peripheral to the right. It is constitutive of it.

The CJEU has reinforced this structural role. Over two decades, the Court has consistently interpreted "personal data" broadly, emphasising the need to ensure effective and complete protection of fundamental rights. In cases such as *Breyer* and *Nowak* (C-434/16), the Court treated identifiability as a contextual but expansive notion, evaluating whether identification is reasonably possible in light of all means likely to be employed, thereby eschewing rigid formalism in favour of a functional approach.

GDPR and the Mutual Reinforcement of Primary and Secondary Law

A defining feature of the GDPR is its deep alignment with EU primary law, understood as a "normative circle": a structural relationship where primary and secondary law mutually reinforce each other, rather than following a simple top-down hierarchy.

In the post-Lisbon legal landscape, Article 8 CFR and Article 16 TFEU provide a constitutional mandate for data protection. The GDPR translates these abstract rights into concrete regulatory provisions. The relationship is thus mutually constitutive: primary law informs the interpretation of the GDPR, while the GDPR, through its detailed provisions, gives concrete expression to Charter rights.

This reciprocal relationship is exemplified by the concept of personal data: anchored in Article 8(1) CFR, it is operationalised in Article 4(1) GDPR, whose broad, inclusive definition gives texture and specificity to fundamental rights. Conversely, Article 23 GDPR explicitly links restrictions on data subjects' rights back to Article 52(1) CFR, constraining regulatory discretion.

In this scenario, the GDPR could be understood not as an ordinary legislative act but as a "quasi-constitutional" instrument within the EU legal order. Here, "quasi-constitutional" does not denote formal hierarchy but functional supremacy, reflecting the GDPR's role as a rights-structuring instrument whose principles influence adjacent legislation. This approach sees it as a distinct normative category, based on its deep connection with Article 8 CFR and its role in giving effect to Article 16 TFEU.

Article 16 TFEU broadly framed language reflects its foundational function of encompassing all human activities that involve some form of personal data processing. Hence, the GDPR is not simply a legislative instrument to be weighed against others of the same rank using traditional interpretative principles. Rather, the GDPR may be conceived as the normative and functional articulation of Articles 8 CFR and 16 TFEU, operating not merely as secondary legislation but as a primary mechanism through which constitutional principles are given concrete effect. This confers upon it a privileged interpretive authority, particularly with respect to its core definitional provisions, even while it remains formally classified as a regulation.

From this perspective, when the GDPR overlaps with other legislative acts, these tensions are resolved not merely through traditional interpretative principles reasoning. Instead, the GDPR is treated as quasi-constitutional status, alongside the Treaties and the CFR, guiding the interpretation of subsequent legislation to preserve the normative core of the fundamental right to data protection.

Why Redefinition Is Not Neutral. The Digital Omnibus as a Constitutional Test Case

Legislative amendments to definitional clauses are often presented as mere clarifications, aimed at crystallising the natural evolution of a concept through jurisprudence and administrative practice. Nonetheless, when a definition shapes the scope of a constitutional right, such "clarifications" are rarely neutral.

Redefining "personal data" alters who falls within the protection of Article 8 CFR. A narrower concept could exclude certain processing activities from constitutional scrutiny altogether. It does not merely adjust compliance burdens. It reshapes the architecture of rights.

Moreover, codifying context-sensitive judicial reasoning into rigid statutory language can create the illusion of precision while sacrificing flexibility. Constitutional adjudication depends on open-textured concepts that allow adaptation to technological change. Freezing a particular judicial formulation into legislative text risks transforming a dynamic interpretive standard into a static rule. In constitutional systems, scope is substance. The boundary of a right often determines its practical force. The definition of personal data is precisely such a contour.

These structural considerations place recent reform initiatives in a different perspective. Within the Commission's Digital Omnibus initiative, amendments to the GDPR have been contemplated in response to perceived enforcement and interpretation challenges. The Commission Staff Working Document accompanying the Digital Omnibus Regulation Proposal identifies persistent difficulties in ensuring consistent application of the GDPR across the Union. It emphasises "the need for a more harmonised and consistent interpretation" of the Regulation, with the aim of reducing fragmentation and promoting uniform enforcement. Among the areas identified as requiring clarification is the definition of "personal data," a particularly disputed aspect of the proposal.

In this context, particular attention has been given to recent case law of the Court of Justice of the European Union, notably the judgment in *SRB* case (C-413/23 P, 4 September 2025). The Staff Working Document notes that stakeholders have called for greater legal certainty regarding the scope of personal data in light of this ruling, which considered whether pseudonymised data remain personal when transferred to a recipient without re-identification means. The Court applied a relative approach, assessing identifiability based on the means reasonably available to the recipient and the surrounding legal and factual circumstances.

Transposing such reasoning directly into Article 4(1) GDPR may appear, like in the past, to enhance clarity. However, even where a reform does not purport to redefine the core elements of the notion (e.g., "information", "relating to", "identified or identifiable natural person") the act of clarifying how these elements operate may subtly transform their substance. Adjusting the interpretative parameters of the criterion of identifiability (for instance, by foregrounding the perspective of a specific recipient or by narrowing the assessment of available means, introducing a more subjective approach) may shift the practical boundary between personal and non-personal data. In doing so, it affects not merely the application of the definition, but its effective nature and reach.

This becomes particularly visible in relation to pseudonymised data. The Digital Omnibus discussions reportedly contemplate clarifying that data which have been pseudonymised, and for which the recipient does not possess reasonably available means of re-identification, may fall outside the notion of personal data in that recipient's hands. While pseudonymisation under Article 4(5) GDPR has traditionally been understood as a security measure that reduces risk without altering the data's legal qualification, the proposed clarification seems to support a low-threshold approach to anonymisation.

Such a move must be read against Recital 26 GDPR, which embeds a dynamic, risk-sensitive and relational assessment within the concept of personal data, without fragmenting its scope according to the subjective position of each recipient. If the Omnibus reform were to crystallise a recipient-relative approach in the operative definition itself, it risks isolating the assessment to the immediate holder of the data, thereby narrowing the material scope of protection even where identifiability persists at systemic level.

Moreover, the proposed Digital Omnibus do not appear to consider the entirety of the Court's reasoning in SRB. The proposal seems to extract and generalise only certain elements of that reasoning (notably the recipient-oriented perspective) without fully incorporating the Court's broader safeguards and contextual limitations. Following the Court's reasoning, identifiability requires an objective, context-sensitive assessment, rather than one limited to the subjective perspective of a particular actor.

Clarification or Recalibration?

If the proposed amendment narrows the circumstances under which data qualify as personal, its implications extend far beyond technical regulation. Such a change would not merely codify case law; it would recalibrate the material scope of Article 8 CFR through secondary legislation, raising profound constitutional questions.

The issue is whether the EU legislature may alter the constitutional perimeter of the right by modifying the concept that defines its reach, particularly through procedural vehicles designed for simplification rather than rights-sensitive reform. Recognising the quasi-constitutional status of this definition does not render it immutable, but it does demand heightened scrutiny.

What appears as a technical clarification may in fact redraw the scope of Article 8. Contextual and relational assessments, including the treatment of pseudonymised data, can shift EU data protection from a universal framework with differentiated obligations to a fragmented one. Scope is not administrative detail; it is constitutional design. The definition of personal data is woven into the Union's constitutional fabric, and it cannot be lightly rewoven.

Pablo Trigo Kramcsák is a doctoral researcher at the Research Group on Law, Science, Technology & Society (LSTS) of the Vrije Universiteit Brussel (VUB), where he is also a legal researcher at the Cyber and Data Security Lab (CDSL) and a fellow at the Brussels Privacy Hub (BPH).

Barbara Lazarotto is a legal researcher at the Law, Science, Technology and Society Research Group (LSTS) of Vrije Universiteit Brussel (VUB) and the Managing Director of the Brussels Privacy Hub, an academic research center associated with LSTS.