EDRi

Assessment of the first draft: Council compromise on the Digital Omnibus (GDPR and ePrivacy)

Analysis and Recommendations

Introduction

A draft compromise text on the GDPR and ePrivacy -related elements of the Digital Omnibus has recently emerged in the Council discussions. Compared with the European Commission's original proposal, the text reflects a significant shift. Several amendments that would have affected core structural elements of the GDPR appear to have been removed, including changes to the definition of personal data, the definition of scientific research, the architecture of Article 22 on automated decision-making, and the proposed implementing powers of the Commission on pseudonymisation.

These developments are welcome. They preserve key safeguards of the GDPR and reduce some of the most significant risks identified in the Commission proposal. **At the same time, the draft text still introduces a number of modifications that could affect how important safeguards are interpreted and applied in practice. In addition, several new problematic provisions introduced in the Commission proposal appear to remain under discussion**

This document analyses the draft compromise text and sets out recommendations to ensure that the ongoing negotiations strengthen, rather than weaken, the protection of personal data, pivacy and fundamental rights as a whole in the European Union.

DELETIONS: preserving core safeguards

ARTICLE 4a: Redefinition of personal data

Status in compromise: deleted (Recital 27 is also deleted, a new Recital 27a is added)

Legal effect:

- The GDPR definition of personal data remains unchanged.
- Identifiability continues to be assessed under Article 4(1) and Recital 26.
- The controller-centric approach suggested in the Commission proposal disappears.
- The new Recital still risks encouraging an overly broad interpretation of the relative concept of personal data. In complex data ecosystems, pseudonymised datasets often remain realistically identifiable through correlation, enrichment, or data sharing across actors. Guidance on pseudonymisation should therefore focus on risk reduction and safeguards rather than suggesting that pseudonymised data may systematically fall outside the scope of the GDPR (see below).

Recommendation: Reject any reopening, including additional Recitals.

The proposed amendment to the definition of personal data is presented as a clarification intended to reduce fragmentation in the interpretation of the GDPR. In reality, it risks producing the opposite effect. The definition of personal data determines when the fundamental right to data protection applies and therefore when the safeguards of the GDPR become operational. Altering this concept would have structural consequences for the coherence of EU data protection law. Rather than resolving fragmentation, the proposal risks introducing new forms of legal uncertainty across the digital economy and across the Union.

1. The definition of personal data determines the scope of a fundamental right

The definition of personal data is not a technical provision. It determines when the fundamental right to data protection becomes applicable and therefore when the entire system of safeguards under the GDPR applies.
Changing this concept affects the threshold of EU data protection law itself. Such a modification cannot be treated as a simple clarification or simplification exercise.

2. The proposal risks increasing fragmentation rather than reducing it

It has been argued that different interpretations of the concept of personal data by supervisory authorities create fragmentation across the Union. The truth is that the proposed solution would itself introduce fragmentation. By making the qualification of data depend more heavily on the capabilities or position of a specific controller, the same dataset could be considered personal data for one actor but not for another.
This would undermine the uniform application of the GDPR and create legal uncertainty for organisations, regulators and individuals alike.

3. The proposal ignores the realities of data processing chains in the digital economy

Modern digital systems rarely involve a single actor processing data in isolation. Data typically move through complex chains involving multiple controllers, processors and sub-processors. Under the proposed approach, different actors within the same processing chain could reach different conclusions about whether the same dataset qualifies as personal data. One controller might treat the information as personal data and apply the GDPR, while another actor in the chain might conclude that the GDPR does not apply. This would create a fragmented regulatory environment across a single processing ecosystem and significantly complicate compliance.

In complex digital ecosystems involving multiple controllers, processors and intermediaries, the same dataset may circulate across several actors. If identifiability is assessed solely from the perspective of each individual actor, the same information could simultaneously be treated as personal data by some actors and as non-personal data by others.

4. The proposal would make compliance more complex rather than simpler

If the qualification of data varies depending on the actor processing it, organisations would need to constantly classify and track datasets according to whether they are considered personal data for each participant in the processing chain. Datasets might be labelled differently depending on context, technical capacity or contractual arrangements. When data are combined, transferred or reused, organisations would need to reassess their classification repeatedly.

Instead of simplifying compliance, this would introduce additional operational complexity and increase the likelihood of disputes and litigation. It would also reinforce structural asymmetries in the digital economy, as large actors with greater technical and legal resources would be better placed to navigate or challenge these classifications, while smaller organisations would bear the uncertainty and compliance burden.

5. The proposal misinterprets the case law it relies on

The proposal is often justified by reference to recent case law of the Court of Justice, in particular the judgment in EDPS v SRB (albeit only one narrow specific section). However, that judgment addressed a very specific factual situation and cannot be interpreted as a general redefinition of the concept of personal data. Elevating reasoning developed in a narrow factual context into a general legislative rule governing the scope of the GDPR would go far beyond what the Court examined.

6. The proposal risks weakening the coherence of the EU legal framework and international standards

Because the definition of personal data determines the material scope of Articles 7 and 8 of the Charter, any reinterpretation of identifiability must be assessed under the conditions of Article 52 of the Charter. Moreover, the GDPR definition of personal data functions as a baseline across the EU digital rulebook. Multiple legislative instruments rely on this concept when determining scope and safeguards. Altering the definition would therefore have cascading effects across other regulatory frameworks. It will also create tension with the broader international understanding of personal data reflected in the Council of Europe Convention 108 framework, which the EU and its Member States support.

While clearer guidance on pseudonymisation techniques should contribute to legal certainty for controllers, the definition of personal data cannot be simplified in a way that artificially narrows the scope of the GDPR. In complex data ecosystems, identifiability often depends on the broader environment in which data circulate rather than on the capabilities of a single actor. Guidance should therefore focus on clarifying safeguards and risk mitigation rather than establishing criteria that allow certain actors to treat pseudonymised datasets as non-personal data.

ARTICLE 41a: Commission implementing acts on pseudonymisation

Status in compromise: deleted (Recital 27 is also deleted)

Legal effect:

- The Presidency deletes the Commission proposal that would have empowered the Commission to adopt implementing acts defining technical criteria for pseudonymisation. The Commission therefore does not gain new regulatory powers over this concept.
- The legal status of pseudonymised data remains unchanged. Under Article 4(5) GDPR and Recital 26, pseudonymised data remain personal data as long as a natural person can still be identified using means reasonably likely to be used.
- However, the issue reappears later in the proposal through the modification of Article 70. The Council introduces a new task allowing the EDPB to issue guidance on pseudonymisation and identifiability, including criteria for assessing when pseudonymised data may no longer constitute personal data for certain entities (see below).

Recommendation: Reject any reopening.

ARTICLE 4(38): Definition of scientific research

Status in compromise: deleted (Recital 28 is also deleted).
The Commission had proposed expanding the definition of scientific research in Article 4.

Legal effect:

- The Presidency text removes this change, so the GDPR definition of scientific research remains unchanged.
- The existing interpretation of scientific research, as reflected in the GDPR and Recital 159, continues to apply.
- As a result, commercial activities such as AI development or large-scale data analytics cannot rely on a broader definition introduced through the Omnibus.
- Why reopening the definition would be problematic:

    - The notion of scientific research in the GDPR plays a structural role because it triggers several derogations and flexibilities in the Regulation.
    - Expanding or redefining the concept would therefore automatically broaden the scope of those derogations, including exemptions from purpose limitation, storage limitation, and certain transparency obligations.
    - Even introducing additional safeguards would not address this structural effect, because the expansion of the definition itself would allow more actors and activities to rely on those derogations.
- In practice, reopening the definition would risk enabling commercial data reuse, including for AI development, to be framed as scientific research in order to benefit from these flexibilities.

Recommendation: Reject any reopening of the definition of scientific research.

- Maintaining the current framework preserves the balance established in the GDPR between facilitating legitimate research and ensuring that the derogations attached to research remain narrowly interpreted.

ARTICLE 22: Automated decision-making

Status in compromise: deleted (Recital 38 is also deleted).
The Commission proposed rewriting Article 22 to weaken its structure.

Legal effect:

- The Presidency deletes this amendment, meaning that Article 22 remains unchanged in the GDPR.
- The current structure of the provision is preserved, including the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects.
- The Commission's proposal would have modified the scope of the 'contractual necessity' exception, potentially allowing automated decisions to be justified more easily in contractual contexts.

Recommendation: Reject any reopening.

MODIFICATIONS: Targeted changes that risk weakening safeguards

ARTICLE 5(1)(b): Purpose limitation

Council modification:

- First change: add the phrase 'subject to the application of appropriate safeguards';
- Second change: delete the wording 'purposes, independent of the conditions of Article 6(4)'.

Legal effect:

- The Commission proposal attempted to allow certain processing purposes outside the compatibility test of Article 6(4). The Presidency removes that possibility.
- Meaning: Further processing must still respect the compatibility framework of Article 6(4).
- However, by adding 'appropriate safeguards' the Council introduces a vague condition that could still be interpreted flexibly. The notion of 'appropriate safeguards' cannot replace the compatibility assessment required under Article 6(4). If interpreted broadly, this language could allow controllers to justify secondary uses of data on the basis of generic technical or organisational measures rather than demonstrating that the new purpose is genuinely compatible with the original one. This risk is particularly visible in the context of AI development, where controllers increasingly attempt to treat the 'training' of AI systems as a separate processing purpose. However, training an AI system is intrinsically linked to the purpose for which the system is deployed, and treating training as an independent purpose risks undermining the purpose limitation principle.

Recommendation: Reject any reopening.

ARTICLE 9: Special category data

Council modification: Amendments remain, but the Presidency tightens them.

First: Article 9(2)(k) and 9(5) (AI training data)

Related to Article 4a AI Act – Use of Sensitive Data for AI systems. Recital 33 is not changed.

The Council adds a safeguard clause requiring controllers to:

- Implement organisational and technical measures to avoid collecting special categories of data;
- Remove this data if detected;
- Protect such data if removal requires disproportionate effort.

Legal effect:

- The derogation allowing the use of special categories of data in AI systems remains in place.
- The Presidency introduces a sequence of obligations intended to limit the risks associated with that derogation:
  - Controllers should first avoid collecting such data where possible;
  - If collection occurs, they must remove the data;
  - If removal is not possible, technical and organisational safeguards must be applied.
- This creates a structured approach that moves from prevention to correction and finally to mitigation.
- While this sequence is stricter than the Commission proposal, it does not eliminate the core issue: sensitive data may still be processed and remain within AI systems under certain conditions.
- As a result, the provision continues to permit the presence and potential use of sensitive data in AI systems, rather than ensuring that such data are excluded from the outset.

Recommendation: Reject any change to the Commission proposal.
Even with the additional safeguards introduced by the Presidency, the provision continues to allow sensitive data to remain within AI systems. Given the heightened risks associated with the processing of special categories of data under Article 9 GDPR, maintaining the Commission text provides a clearer and more protective approach.

Second: Article 9(2)(l) (biometric authentication)

Council modification: Recital 34 is changed. The Council introduces three modifications:

- adds 'one-to-one verification';
- adds 'and possession' of the data subject;
- adds requirement that processing must be authorised by EU or Member State law with safeguards.

Legal effect:

- These changes attempt to narrow the derogation by framing biometric processing primarily as an authentication tool. The references to 'one-to-one verification' and 'possession' seek to distinguish authentication from broader forms of biometric identification or tracking.
- The additional requirement for a legal basis in Union or Member State law introduces a formal safeguard intended to ensure that biometric processing is subject to democratic oversight.
- However, the core derogation remains in the Regulation. Once a specific exception allowing biometric authentication is embedded in Article 9, it risks normalising the use of biometric systems in digital services. In practice, providers may increasingly treat biometric verification as a standard authentication method rather than an exceptional measure.
- Even with the additional conditions, the provision could still encourage wider deployment of biometric systems across the digital economy, including in contexts where less intrusive authentication methods would be sufficient.

Recommendation: Reject any change to the provision. Maintaining the current framework avoids creating a specific legal pathway that could accelerate the normalisation of biometric authentication in everyday digital services.

ARTICLE 12(5): Limitation of the right to access

Council modification: Recital 35 is changed.
The Presidency modifies the Commission text rather than deleting it.

Key changes:

- replaces 'and, in the case of' with 'or also, for';
- introduces the phrase 'where an abusive intention on the part of the data subject can be demonstrated';
- deletes the 'reasonable grounds to believe' formulation;
- adds 'or that the request is submitted with an abusive intention'.

Legal effect:

- Controllers may refuse requests where abusive intention can be demonstrated.
- Compared with the Commission proposal:
  - the wording is more precise;
  - but the concept of abuse remains → setting a dangerous precedent, the GDPR introduces an explicit concept of abuse of rights in access procedures.
- So the Presidency keeps the new refusal ground but tightens the formulation slightly. This directly affects how Articles 15–22 are exercised.

Recommendation: Reject any change to the provision.

If the provision remains open for negotiation → strict safeguards to prevent misuse of this clause.

In line with the EDPB/EDPS Opinion, refusals based on abusive intention should:

- require clear and demonstrable evidence;
- be reasoned and documented;
- be subject to review by supervisory authorities;
- explicit confirmation that access requests do not require justification.

The provision should explicitly clarify that broad or exploratory requests cannot be considered abusive, given the inherent information asymmetry in data processing.

Specific wording: add '*A request shall not be considered excessive or abusive solely because the data subject does not provide a justification for the exercise of their rights.*'

Insert the following sentence: '*a request shall not be considered abusive solely on the basis that it is broad, exploratory, or submitted with the aim of verifying the lawfulness of processing. Any refusal on the grounds of abusive intention shall be reasoned, documented, and communicated to the data subject without undue delay.*'

ARTICLE 13(4): Exemption from information obligations

Council modification: Recital 36 is changed. The Council rewrites several elements.

- adds requirement that the data subject must actually have the information
- clarifies that the relationship must be 'clear';
- replaces the 'data-intensive' criterion with a detailed description of high-risk processing;
- adds that the exemption does not apply if the controller intends to process data for other purposes.

Legal effect:

- The Presidency tries to limit the exemption to low-risk processing contexts
- It also reintroduces a safeguard against purpose expansion.
- So compared to the Commission proposal, the exemption becomes narrower.
- The exemption for information duties becomes more structured and limited to low-risk contexts. Transparency obligations are relaxed for simple relationships but restored when processing expands or becomes complex.

Recommendation: Reject any change to the provision.
If the provision remains open for negotiation → ensuring that transparency remains the default rule.
The exemption should apply only where all of the following conditions are met:

- the relationship between controller and data subject is clearly defined;
- the processing is low-risk;
- the processing remains limited to the original purpose.

Controllers should be required to provide information as soon as processing becomes more complex or involves automated decision-making, profiling, or data sharing.

Specific wording: Modify the exemption clause: '*the obligations referred to in paragraphs 1 to 3 shall not apply where, and insofar as, the data subject demonstrably already possesses the information and where the processing takes place within a clear and limited relationship and is unlikely to result in a high risk to the rights and freedoms of natural persons.*'
AND add safeguard sentence: '*The controller shall bear the burden of demonstrating that these conditions are fulfilled.*'

Objective: Prevent controllers from presuming knowledge without evidence.

ARTICLE 13(5): Research exemption to information obligations

Council modification: Recital 37 is changed. The Council clarifies that the exemption only applies when:

- the same controller performs further processing for research;
- safeguards under Article 89(1) apply.

Legal effect:

- This restores some of the safeguards removed in the Commission version.

Recommendation: Reject any change to Article 13(5).
If the provision remains open for negotiation, the following safeguards should be introduced:

- Maintain the Presidency clarification that the exemption only applies when the same controller carries out the research processing and Article 89(1) safeguards apply.
- Limit the exemption strictly to situations where providing the information would render the research impossible or seriously impair the research objectives.
- Require controllers relying on the exemption to document and justify the necessity of the exemption and make this assessment available to supervisory authorities.
- Ensure that alternative transparency measures remain mandatory, such as publicly accessible information about the research processing.
- Clarify that the exemption cannot be used for large-scale commercial data reuse, including analytics or AI training.

ARTICLE 35: Data Protection Impact Assessments

Council modification: Recital 40 slightly changed. The Commission proposal would have given the Commission implementing powers over high-risk processing lists. The Presidency deletes that approach. Instead:

- Supervisory authorities establish and publish their own lists;
- The Commission no longer adopts implementing acts.

Legal effect:

- Control returns to DPAs and the EDPB rather than the Commission. The shift from Commission implementing acts to EDPB guidance addresses concerns about delegating interpretive authority over core GDPR concepts to the Commission. However, guidance cannot redefine the material scope of the Regulation, and the distinction between technical clarification and substantive reinterpretation must remain clear.
- Paragraphs 6a and 6b are deleted.
- Paragraph 6c remains but refers to lists established by the Board.

Recommendation: Welcome the removal of Commission implementing powers but recommend strong coordination through the EDPB.

Specific wording: Add clarification to the provision on lists: '*the establishment of lists of processing operations that do not require a data protection impact assessment shall not exempt controllers from the obligation to assess the risks arising from the specific design, scope, context, and purposes of the processing.*'

Objective: Prevent DPIA lists from becoming blanket exemptions.

ARTICLE 70(1): Tasks of the EDPB

Council modification: Multiple modifications occur. The Board now:

- establishes lists of high-risk processing
- establishes lists of low-risk situations
- establishes criteria for DPIA obligations

The Presidency also adds a new task (hca): this task allows the Board to issue guidelines on pseudonymisation and identifiability, including criteria to determine when pseudonymised data may no longer be personal data.

Legal effect:

- Although Article 41a was deleted, the Council reintroduces the issue through guidance rather than implementing acts
- This shifts the role from the Commission to the EDPB.

Recommendation: clear limits to this mandate.
Guidance on pseudonymisation should reaffirm that pseudonymised data remain personal data under the GDPR. The EDPB's guidance should not create new legal categories that would allow certain actors to treat pseudonymised data as non-personal.

Specific wording for the new subparagraph: Replace with: '*issue guidelines, recommendations and best practices on pseudonymisation, clarifying the circumstances in which a natural person is identifiable and the means reasonably likely to be used for identification, in accordance with Article 4(1) and Recital 26. Such guidance shall reaffirm that pseudonymised data remain personal data unless identification, including singling out, of the data subject is no longer reasonably possible.*'

Objective: Prevent reinterpretation of pseudonymised data as non-personal data.

ARTICLES 88a, 88b and 88c (and Article 5(3) ePrivacy): New provisions, structural risks that must be addressed

Council modification: The Presidency compromise does not yet modify these provisions

Article 88a and b

Recommendation: Accept the Commission's proposal provided that the provisions remain within the framework of the ePrivacy Directive and incorporate the safeguards outlined below, in order to prevent loopholes through exemptions and to ensure that privacy signals are legally effective and binding from the outset.

- The confidentiality of communications framework established by the ePrivacy Directive must not be weakened through the Digital Omnibus. Sector-specific protections remain necessary alongside the GDPR and should remain the primary legal framework governing access to communications data and terminal equipment.

- The substance of proposed Articles 88a and 88b should remain within the ePrivacy framework, for example through amendments to Article 5(3), preserving the logic of confidentiality of communications and terminal equipment integrity.

- Limited clarifications or targeted broadening of exemptions may be acceptable where strictly necessary and proportionate. Any such exemptions should follow the approach previously agreed by the European Parliament in the ePrivacy Regulation negotiations and include strict technical safeguards, narrow purposes, and short retention periods.

- Consent-free device access allowances, including for audience measurement or security, must include enforceable technical constraints. These should include strict purpose limitation, bans on persistent identifiers and fingerprinting, short retention periods, and explicit prohibitions on reuse, profiling, repurposing, or AI training.

- Privacy signals should be defined in law and recognised as legally valid expressions of refusal of non-essential tracking. Signals that meet the legal requirements of the framework should be mandatory and binding from the outset, rather than subject to long transitional periods.

- Signals that already function in practice, such as browser-level refusal signals, should be recognised immediately as valid expressions of refusal where they clearly convey the individual's choice.

- Privacy signals must operate across the full technical stack. Legal obligations should therefore apply not only to browsers but also to operating systems, application environments, and other user agents, since a large share of tracking occurs through apps, SDKs, and OS-level identifiers.

- Technical standards should ensure interoperability and consistent interpretation of signals across web and app contexts, while preventing vendor lock-in and allowing third-party privacy tools to generate and manage signals on behalf of users.

- Privacy signals must not require persistent identifiers or device-level markers in order to be recognised. Implementation should avoid creating new tracking layers designed to remember consent choices.

- The law should define the key elements required for signals to function effectively, including clear semantics, scope by context, lifecycle symmetry including withdrawal, and verifiability obligations for controllers. The interpretation of these elements and the limits of the standardisation process should be guided by the European Data Protection Board to ensure that technical standards remain aligned with fundamental rights and the objectives of Union law.

- Privacy signals should apply universally across the digital ecosystem. Sectoral exemptions, such as those proposed for media actors, and carve-outs based on company size are incompatible with a fundamental rights framework and undermine legal certainty.

- The introduction of privacy signals must not create new exceptions to the rules governing access to terminal equipment or the confidentiality of communications.

Article 88c (and Recitals 30 and 31) on AI systems

Recommendation: Deleting this provision entirely.

- The GDPR should remain technologically neutral. Introducing a specific lawful basis for AI development risks creating a presumption that large-scale data reuse for AI is legitimate. Existing lawful bases already provide sufficient flexibility when applied correctly.