CM2604

MEIJERS COMMITTEE COMMENT ON THE DIGITAL OMNIBUS PROPOSAL

FEBRUARY 2026

The Meijers Committee warns that the Digital Omnibus proposals introduce substantial changes to EU data-protection and AI law that could weaken fundamental rights. Despite their effect on fundamental rights, the proposals were introduced without an impact assessment on privacy and data protection.

The Committee is particularly concerned about:

- the redefinition of personal data, which allows controllers to treat pseudonymised data as non-personal if they lack the means to re-identify individuals. This creates inconsistent standards and contradicts CJEU case law;
- the expanded legal bases for AI development, which allows AI developers to rely on "legitimate interest" rather than consent to process personal data for AI training. This could normalize broad data use without adequate necessity or proportionality checks;

Meijers Committee

Standing committee of experts on international immigration, refugee and criminal law

- the weakened protection of sensitive data, where special category data remains in AI training datasets if removal is "too difficult". This contradicts CJEU case law which requires strict interpretation of exceptions to the prohibition on processing such data;
- the introduction of changes to the AI Act, which raises concerns about large-scale collection of sensitive data to detect or correct AI bias. It also delays high-risk AI obligations and abolishes public registration for certain high-risk systems, which reduces transparency and oversight;
- the restrictions on data subject rights, which would make it harder for individuals to understand or challenge data processing. This undermines rights under the Charter.

The Meijers Committee therefore urges the legislators to conduct a full fundamental rights impact assessment and remove the proposed amendments concerning the definition of personal data, the expanded ground for AI development, the processing of sensitive data, and the restriction of data subject rights.

Meijers Committee

Standing committee of experts on international immigration, refugee and criminal law

Meijers Committee

1. Introduction

On 19 November 2025, the European Commission published its Proposal for a Regulation, also known as the Digital Omnibus proposal.[1] Following the Commission's communication on a simpler and faster Europe[2] and the European Council's conclusions calling for further simplifying and consolidating legislation,[3] the Digital Omnibus proposal is accompanied by a Digital Omnibus on AI proposal[4] aiming to simplify digital EU legislation, including the General Data Protection Regulation (GDPR), the ePrivacy Directive and the Artificial Intelligence (AI) Act.

In principle, the Meijers Committee welcomes efforts to clarify existing legislation but emphasizes that this should not result in weakening citizens' fundamental rights. For that reason, we bring forward four main points of concern where fundamental rights are negatively affected by the proposed amendments and procedure, namely about a fundamental rights impact assessment; defintion of personal data; AI systems; and rights of data subjects.

2. Fundamental Rights Impact Assessment

The Digital Omnibus proposal and the Digital Omnibus on AI proposal are introduced without a full impact assessment report. In the explanatory memorandum of both proposals, the Commission refers to the amendments as targeted and technical in nature, designed to ensure a more efficient implementation of the rules, to justify this choice. However, the proposals go much further than that and, thus, require an impact assessment. Impact assessments are required when initiatives are likely to have significant economic, environmental or social impacts or entail significant spending.[5] The explanatory memorandum of the Digital Omnibus proposal includes a short section claiming to address fundamental rights,[6] but it focuses almost entirely on the supposed right to conduct a business. This is a one-sided reading of the Charter of Fundamental Rights and Freedoms primarily championing economic rights. The memorandum does not explain how the changes would preserve a high level of data protection nor how individual fundamental rights would remain safe once key safeguards are weakened. The Meijers Committee stresses the need for fundamental rights impact assessments as a key instrument of better regulation. A conscientious legislative process is needed to allow for time to consider the legal and practical consequences of the proposed changes.

3. Definition of Personal Data

The Meijers Committee is concerned by the redefinition of personal data,[7] which seems to exclude certain pseudonymised data from the scope of the GDPR. The proposed change weakens the current rule that information counts as personal data if it could reasonably be used to identify a person. With

[1] 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 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024, COM(2025) 837 final.
[2] COM(2025) 47 final.
[3] European Council, Conclusions, EUCO 1/25, 20 March 2025.
[4] COM(2025) 836 final.
[5] European Commission, Better Regulation Guidelines, SWD(2021) 305 final, 3 November 2021, p. 30.
[6] Explanatory memorandum, p. 15.
[7] Article 4(1) GDPR.

the proposed change, organisations would be allowed to say that some information is not personal data if they claim they do not have the means reasonably likely to identify anyone from it, even if others could. This introduces a subjective approach to the definition of personal data.[8] Some organisations could classify the same data as personal while others as non-personal, resulting in the data not being covered by the GDPR. Such approach has a detrimental effect on legal certainty and the uniform application of EU law. This could mean that data subjects cannot exercise their rights under the GDPR.

The Meijers Committee stresses, referring to guidelines of the European Data Protection Board (EDPB) in 2025, that pseudonymised data, 'which could be attributed to a natural person by the use of additional information, remains information related to an identifiable natural person, and thus is personal data'. This is why the processing of such data also needs to comply with the GDPR, including the principles of lawfulness, transparency, and confidentiality under Art. 5 GDPR, and the requirements of Art. 6 GDPR.[9]

The CJEU stresses that data which became 'impersonal' through pseudonymisation for the data controllers or certain users, may become 'personal' when put at the disposal of other people or organisations who have means reasonably likely to enable the data subject to be identified.[10] According to the CJEU, 'in so far as it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those third parties. In such circumstances, pseudonymised data should be considered to be personal in nature.'[11] The definition of 'personal data' is a core definition of the GDPR and redefining this term will have consequences for the whole regulation.

Furthermore, the proposal includes the option for the European Commission to adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.[12] This amendment could lead to introducing an independent assessment of the state of the art of the available techniques.[13] Such assessment could be a positive addition as it may offer clarity on those techniques that can or cannot lead to re-identification of the data subjects, especially with the proposed involvement of the EDPB. Nevertheless, the amendment also enables the Commission to create criteria and/or categories for controllers and recipients to assess the risk of re-identification related to typical recipients of data. This amendment potentially places the Commission in a role in which they could exclude specific categories of data or specific (groups of) controllers from the scope of the GDPR.[14] Even if the proposal allows the EDPB to be involved in the aforementioned assessment, it does not give binding force to the opinions of the EDPB. Therefore, the proposal insufficiently ensures that the EDPB will play a safeguarding role against this excluding practice.

[8] See also NOYB, Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the Commission, 2025, p. 5-6.
[9] EDPB Guidelines 01/2025 on Pseudonymisation, Guidelines 01/2025 on Pseudonymisation | European Data Protection Board
[10] CJEU 4 September 2025, C- 413/23 P, paragraphs 83-85.
[11] Ibid, paragraph 85.
[12] See proposed Article 41a.
[13] As mentioned in proposed Article 41a(2).
[14] See also NOYB, Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the Commission, 2025, p. 6.

4. AI Systems

New legitimate interest for AI

The European Commission proposes a new article[15] that allows data controllers to use "legitimate interest" (Article 6(1)(f) GDPR) as the legal ground for processing data for the "development and operation of an AI system". Such a provision would allow for controllers to use data subject's posts, photos, or voice recordings to train AI systems without their individual consent as required in Article 6 (1)(a) GDPR.

The Meijers Committee is concerned by explicitly allowing the use of Article 6(1)(f) GDPR, instead of the aforementioned Article 6(1)(a) as the legal basis for the development and operation of an AI system. The explicit mentioning of this legal basis (Article 6(1)(f) GDPR) could provide the impression that the use of this legal basis is always possible and is preferred, even if the data processing cannot be considered necessary or proportionate.

Sensitive Data

The Meijers Committee is concerned by the added paragraphs to Article 9 GDPR[16] regarding the processing of special categories of personal data (sometimes called sensitive data). The proposed changes add a new legal basis to allow controllers to process special category data for the purposes of the development and operation of AI systems. Although the proposed Article 9(5) GDPR states that controllers are obliged to remove residual special category data, it allows special category data to remain in AI training datasets if its removal is considered too difficult. The proposed change could render the GDPR's rules of special category data largely meaningless in practice as controllers could claim a disproportionate effort by default if large or unstructured data sets are involved. Considering the sensitivity of special category data such a subjective safeguard is insufficient to protect the fundamental right to private life and data protection and the right to non-discrimination.[17] In *Ligue des droits humains*, the CJEU noted that using AI and self-learning risk models may deprive data subjects of their right to an effective judicial protection as protected in the EU Charter of Fundamental Rights , in connection with their right to private life and data protection, but also when challenging the potential discriminatory impact of such models.[18]

Moreover, the Commission has also added a new legal ground for the processing of biometric data for identification where the biometric data stays under the person's control, proposing an amendment of Article 9 GDPR. Such a provision would eliminate the need to comply with explicit consent requirements. Controllers using biometrics for convenience may be able to rely on the proposed legal ground for processing more often, as long as the biometric data remainunder the user's control.

Sensitive data receives a higher protection level in the GDPR as it can reveal or strongly suggest details such as a person's health, sexual orientation, political opinions, religious beliefs, or biometric details used to identify them. Therefore, these special categories of data receive the strongest protection in EU law because its misuse can cause serious harm or result in discriminatory treatment. The proposed amendments will result in a lower level of protection in comparison to what individuals are entitled to also on the basis of their right to private life and data protection. As underlined by the CJEU, in view of the significant risks to the fundamental freedoms and fundamental rights of data subjects arising from

[15] Article 88c.
[16] Article 3(3) of the Digital Omnibus proposal.
[17] Articles 7, 8, and 21 of the Charter.
[18] CJEU 21 June 2022, *Ligue des Droits Humains*, C-817/19, ECLI:EU:C:2022:491, paragraphs 195 and 209.

any processing of personal data falling within the categories referred to in Article 9(1) GDPR, the objective thereof is to prohibit, in principle, such processing, irrespective of its stated purpose.[19] Exceptions to the general prohibition of the processing of these special categories of data must be interpreted strictly. Provisions such as 'under the person's control' include the risk to be interpreted too broadly.[20] Therefore, the Meijers Committee proposes to delete this amendment.

AI Act

The European Commission's proposal also amends the AI Act, which was adopted on 13 June 2024 and has not fully entered into force yet. The proposal adds a new article[21] which allows for companies to process special categories of data to detect or correct bias in AI systems.

Allowing providers and deployers of AI systems to exceptionally process special categories of data to detect or correct bias in AI systems comes with significant risks. Even if the proposed Article 4a provides in additional conditions for the providers and deployers of AI systems to safeguard such processing of special categories of data, it is essential that this remains the exception rather than the rule. In addition, it is important to have independent supervision on this type of processing. The new article[22] brings the risk that providers and deployers of AI collect special categories of data on a massive scale. Such data collection comes with many risks.[23]

Moreover, the European Commission proposes to delay the implementation of rules for high-risk AI systems. This amendment reduces the urgency for providers and users to take protective measures and creates considerable uncertainty: if the omnibus cannot be adopted before August 2, 2026, the high-risk requirements will apply from that date onwards and may then be temporarily suspended again.

Furthermore, the proposal abolishes the public registration requirement for certain AI systems that fall under the high-risk category that do not pose a significant risk to health, safety, or fundamental rights. The current AI Act exempts AI systems from the specific (product-) requirements for high-risk AI systems, but these systems are still subject to a public registration requirement. Even if this placed the responsibility on the systems' developers, it was at least clear that the provider had used this exemption and that the AI system does not carry a CE mark. This registration requirement is now abolished in the proposed Omnibus AI. Potentially risky systems will therefore fall outside the public and supervisory authorities' view, increasing the risk of dangerous incidents.

5. Rights of Data Subjects

The European Commission proposes changes in the data subjects' rights under the GDPR. The proposed change in Article 15 GDPR allows for controllers to deny the right to access of data subjects when there

[19] CJEU 4 July 2023, C-252/21, *Meta Platforms Inc*, paragraphs 70-73.
[20] See in comparison addressing the definition of 'manifestly made public by the data subject' in Meta Platform Incl, where the CJEU emphasizes in paragraph 84, that Article 9(2)(e) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories set out in Article 9(1) of the GDPR relate, the user does not manifestly make public, within the meaning of the first of those provisions, the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies.
[21] Article 4a.
[22] Ibid.
[23] Van Bekkum, Marvin, and Frederik Zuiderveen Borgesius. "Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?." *Computer Law & Security Review* 48 (2023).

are reasonable grounds to believe that the request is excessive. Furthermore, the amendment provides that data subjects only use their right to access for data protection purposes, excluding journalistic, research, political, economic, legal or other purposes to access personal data. The proposal requires that the data subject must submit a request for access as specifically as possible. The proposal would restrict the data subject's right, as it would make it more difficult for data subjects to exercise their right when they do not necessarily know what personal data is processed by an organisation.

Furthermore, the proposed change in Article 13(4) GDPR allows companies to skip detailed explanations if they believe the person already knows what is happening, or if they consider the relationship as clear enough. The proposal allows for controllers to publish generic statements instead of notifying individuals directly when they process data for scientific purposes.[24] The term scientific research was not included in the definitions under Article 4 GDPR. It is valuable to introduce a definition, however the definition in the proposed Article 4(38) is not limited to research for scientific purposes but also includes research done for commercial purposes. Such a wide approach combined with the aforementioned proposed amendment would make transparency optional.[25] Without clear information, citizens will struggle to understand or challenge what happens to their data. Considering that the protection of the purpose limitation principle does not apply to data processing solely for research purposes, this amendment will weaken the effectiveness of every other data subject's right in the GDPR.

The Meijers Committee stresses that the right in Article 15 GDPR is closely connected to the right not to be subjected to automated decision-making in Article 22 GDPR and the right to effective judicial protection in Article 47 of the Charter. Limiting the right to access to personal information of the data subject, risks undermining these rights.[26]

The proposal also includes changes to article 22 GDPR, on the right of the data subject not to be subject to a decision based solely on automated processing, including profiling. The proposal would seriously weaken Article 22 GDPR. The proposed amendment, replacing the first two paragraphs of Article 22, turns the right of the data subject into an opportunity for the data controller who could base a decision affecting the data subject solely on automated processing including profiling, when that decision fulfils one of three conditions. This amendment effectively results in the removal of the right of the data subject not to be subject to a decision based solely on automated processing. The proposed formulation makes it more difficult for data subjects to exercise their rights against such decision making.

6. Recommendations

Therefore, the Meijers Committee recommends that the EU legislator:

- Complies with the Better Regulation Guidelines by preparing a fundamental rights impact assessment of the Digital Omnibus proposals before continuing with the negotiations;
- Removes the amendment concerning the definition of personal data in article 4(1) GDPR. Should the amendment be kept, the opinion by the EDPB included in proposed article 41a should be made binding;

[24] Article 13(5) GDPR.
[25] See also NOYB, Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the Commission, 2025, p. 33.
[26] CJEU 25 February 2025, C-203/22 *CK v Dun & Bradstreet Austria*, paragraphs 55-58, 73.

- Removes the amendment concerning the use of legitimate interest as a ground for processing data for the development and operation of an AI system in proposed article 88c;
- Removes the amendment concerning the added paragraphs to article 9 GDPR regarding the processing of sensitive data;
- Removes the amendment concerning article 15 GDPR and article 13(4) GDPR;
- Removes the amendment concerning article 22 GDPR.