Council of Bars and Law Societies of Europe
The voice of European lawyers

Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE comments on the proposals for the Digital Omnibus on AI and Digital Omnibus on Data

27 March 2026

The Council of Bars and Law Societies of Europe (CCBE) represents the Bars and Law Societies of 46 countries, and through them more than 1 million European lawyers. The CCBE is recognised as the voice of European lawyers, representing European Bars and Law Societies in their common interests before European and other international institutions. Defending human rights and the rule of law are central values of the CCBE.

Regarding the process

On 19 November 2025, the Commission published the Digital Simplification Package consisting of the Proposal on simplification of the implementation of artificial intelligence rules (Digital Omnibus on AI) and the Proposal on simplification of the digital legislation (Digital Omnibus).

The CCBE echoes the concern of several civil society organisations who pointed out the lack of impact assessments and unrepresentative stakeholder meetings that preceded the publication of the proposals.[1] The CCBE points out that the deadlines for consultations and calls for evidence were very short which made it difficult for a membership-based organisation to effectively engage in the consultation.

Digital Omnibus on AI

Regarding the changes to the processing of sensitive personal data (Article 4a)

The CCBE is concerned about the expansion of the provision on processing of sensitive personal data to providers and deployers 'of other AI systems and models.' In its current form, the provision risks expanding sensitive data processing without adequate necessity tests, proportionality obligations, or independent oversight.

The CCBE also calls for reinstatement of the strict necessity test as contained in the original wording of Article 10(5) of the AI Act. Under the GDPR read in light of the Charter for Fundamental Rights, 'strict necessity' in the context of special categories of data means that such processing

[1] CDT Europe, Digital Omnibus Threatens Hard-Won AI Safeguards, December 2025, page 9 and 10: https://cdt.org/wp-content/uploads/2025/12/CDT-Europe-Brief-Digital-Omnibus-Threatens-Hard-Won-AI-Safeguards.pdf

is allowed only where it is *indispensable* for a clearly defined, legitimate aim, there are no *less intrusive means*, and *specific safeguards* tightly limit and protect the data and the rights of the data subjects.

Furthermore, the CCBE has concerns regarding the change of wording in the new Article 4a(1) which reads that in future, instead of the 'provisions' currently regulated in Article 10 of the AI Act, only the 'safeguards' of the GDPR must be complied with. If interpreted accordingly, this could lead to an excessive reduction in the current level of protection that is incompatible with the fundamental rights guarantees relating to data and privacy protection. The wording 'provisions' should therefore be retained.

Finally, the CCBE stresses that due consideration should be given to the changes proposed under the Digital Omnibus on Data. Those changes, which also concern processing of sensitive personal data, include proposals for changing the definition of 'personal data'. Since the Digital Omnibus on AI refer to 'personal data' and 'sensitive personal data' it follows that any change in the definition of personal data brought about by the Digital Omnibus on data will materially affect the meaning of the relevant provisions in the Digital Omnibus on AI. Given the difference between the respective timetables for negotiations of the Digital Omnibus on Data and the Digital Omnibus on AI, the CCBE calls for a coordinated approach in order to arrive at a coherent solution.

Regarding AI literacy as set out in Article 4

The CCBE urges the co-legislators to maintain the obligations on deployers and providers to ensure sufficient levels of AI literacy. The CCBE equally supports the objective of strengthening AI literacy initiatives at EU and Member State level and recognises the value of coordinated actions by the Commission, including guidance, training programmes and awareness-raising measures. The CCBE stresses that deployers will include public authorities such as courts where the knowledge of the tools used, including AI, their capabilities and limitations is of paramount importance to ensure the proper administration of justice. This is even more important given the recently published Digital Justice Strategy 2030 and Judicial Training Strategy, both of which will require substantial and continuous training efforts, especially in light of the fast pace of technological change.

Regarding the registration obligation set out in Articles 6(4) and 49(2)

The CCBE urges the co-legislators to maintain the obligation to register the AI systems which are listed in Annex III but are not high-risk (following the providers' self-assessment), as set out in Article 49(2). Such systems include the AI systems to be used by law enforcement or the justice system.

The CCBE stresses that this amendment substantially diminishes the transparency of AI systems deployed in the contexts of law enforcement and the administration of justice, which are domains predominantly encompassed within Annex III as high-risk use cases. Examples include systems designed to support judicial authorities in legal research and interpretation, or to inform

law-enforcement decision-making. Even when a provider characterises a tool used by courts, prosecution services, or police as merely "procedural" (such as workflow routing, prioritisation mechanisms, or document-triage functions), such systems can nevertheless exert significant influence on litigation pathways, the framing and assessment of evidence, and the timing or substance of judicial determinations. The CCBE maintains that registration is both a foundational and necessary condition to achieve and ensure valid judicial scrutiny and meaningful supervision.

In this regard, the CCBE echoes the recommendations of the EDPB-EDPS' joint opinion in which it is stated that the registration obligation: '[...] *ensures the transparency and traceability of these systems towards the public as well as the national competent authorities. Given that the AI systems in question could still pose potentially significant risks, the registration obligation does not seem unreasonable or disproportionate*.'

Regarding the implementation date set out in Article 113

The CCBE understands the co-legislators' reasons on why the application of the provisions on high-risk AI systems should be postponed. Nevertheless, the CCBE highlights the fact that AI systems are already being deployed in the field of administration of justice and law enforcement. The CCBE has is concerned that, during the extended transitional period, these systems may continue to operate without the specific safeguards foreseen by the AI Act, such as risk management systems, data governance requirements, human oversight obligations and post-market monitoring.

The CCBE also stresses that this change must be read together with other proposed changes to the AI Act, including the removal of the registration obligation (see above). In this context another key issue is the failure of the proposal to set out any compensatory transparency and accountability mechanisms which should apply during the interim period. When registration and traceability are simultaneously weakened, postponement risks creating a regulatory vacuum precisely in those sectors where fundamental rights are most at stake, including the administration of justice and law enforcement).

The CCBE shares the views of the EDPB-EDPS (joint opinion) which express strong concerns about this change and its impact on the protection of fundamental rights in the fast-changing environment of AI. If the proposed postponement were to go ahead, the CCBE would support the recommendations of the EDBP-EDPS which state that: '*given the different nature of the obligations for providers and deployers of high-risk AI systems laid down in Chapter III, Sections 1, 2, and 3 AI Act, the EDPB and the EDPS invite the co-legislators to consider whether it would be appropriate and feasible to maintain the current timeline for certain obligations, e.g. on transparency*.'

Digital Omnibus on Data

Regarding the conditions for re-use of data held by public authorities (Article 32w, Data Act)

This proposal introduces several new provisions, including Article 32w on the conditions for re-use of data, including certain categories of protected data, held by public authorities. Article 32w(2)(b) refers to data being considered confidential '*in accordance with Union or national law on commercial or statistical confidentiality*.' The other two references are to intellectual property rights and compliance with the GDPR.

This provision could have the effect of making public data held by public authorities, such as courts or ministries of justice. The treatment of such data differs amongst member states. In some jurisdictions, data such as court judgments are available free of charge and the information therein is not redacted or anonymised. In other countries, the opposite is true. Therefore, the CCBE calls for the explicit recognition in the Omnibus on Data of the differing treatment of such data in different jurisdictions along with specific provisions to ensure respect for the relevant national rules that govern the processing and disclosure of such data.

Regarding the definition of personal data (Article 4 GDPR)

The CCBE is concerned that, by the proposed change to the definition of personal data, the Commission goes beyond what is permitted according to case law. In particular, the concept of 'that entity' is too restrictive and contrary to the case law derived from judgment C-319/22, according to which: '[i]n order to determine whether a natural person is identifiable, directly or indirectly, account should be taken of all the means likely reasonably to be used either by the controller, within the meaning of Article 4(7) of the GDPR, or by any other person, to identify that person, without, however, requiring that all the information enabling that person to be identified should be in the hands of a single entity [...]'

The CCBE agrees with the concern expressed by the EDPB-EDPS in their joint opinion that: '*the proposed changes do not accurately reflect and clearly go beyond the CJEU jurisprudence*' and that '*the proposed changes would result in significantly narrowing the concept of personal data, thereby adversely affecting the fundamental right to data protection*.'[2]

As stated above the changes in the definition of personal data have consequences for other parts of the Regulation, as well as other pieces of EU legislation.

If personal data which has been pseudonymised no longer falls within the definition of 'personal data' then, should that pseudonymisation be reversed by technical means, it could lead to a situation where personal data are exposed. One can envisage a situation in which personal data, including sensitive personal data, relating to legal proceedings which have been

[2] EPDB-EDPS Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus): https://www.edps.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf (page 10)

pseudonymised, could lose the status of personal data, thereby no longer benefiting from the protection afforded by the GDPR.

Regarding the processing of special categories of data (Article 9, GDPR)

The CCBE is concerned about the expansion of the possibilities for processing sensitive personal data without sufficient clarifications on the applicability of the principle of proportionality. The proposed change would apply to the development of AI systems *and* their operation. Moreover, the change would allow processing that would otherwise be illegal simply because it is carried out by AI. By favouring one technology over others, the proposal represents a departure from the principle of technological neutrality which underlies the GDPR.

Regarding the right of access to personal data (Article 12 GDPR)

The CCBE stresses that the proposed change to Article 12 constitutes a significant restriction of legitimate rights of access. There is no legitimate reason to restrict the right of access solely to the protection of one's data in the strict sense. In this context, the CCBE echoes the observations of the EDPB-EDPS who pointed out that Article 1 GDPR: '[...] *clearly underlines that the GDPR, and more generally the right to protection of personal data in Article 8 of the Charter, aims to protect all individuals' fundamental rights and freedoms, and is not limited to the protection of personal data alone*.'

Maintaining the proposed wording could result in situations where, for example, an employee uses an access request in the context of a labour dispute and where the employer could reject it as 'abusive'.

Regarding the information to be provided where personal data are collected from the data subject (Article 13(4) GDPR)

The CCBE recommends clarifying the scope of the notions of 'reasonable grounds' and 'not data-intensive', which are too vague and could prevent a large proportion of citizens from exercising their rights of access and rectification.

Regarding automated decision making (Article 22, GDPR)

The CCBE is concerned over the proposed change since it constitutes a fundamental change in the spirit of the provision. The most significant change is that the removal of the wording stating the right not to be subject to a decision based solely on automated processing. The replacement attempts to list the instances where such processing is allowed, largely based on the current text, save for the interpretation of 'necessity.' The proposed change extends the discretion of controllers to use automated decision making whenever judged necessary regardless of whether other options are available. In practical terms, this may result in a more frequent use of such automated systems. This change also makes it more difficult for citizens to exercise their right to

object in practice, as they now bear the burden of proving that the conditions for automated processing have not been met in order to be able to object. Previously, the opposite was true.

In its previous work,[3] the CCBE strongly advocated for the right to a human judge and for the justice system to remain human-centric and now maintains that position.

Regarding the processing of personal data for the purposes of AI training on the basis of legitimate interest

The new Article 88c ensures that the development or operation of an AI system constitutes a legitimate ground for processing personal data, unless another national or European provision stipulates that consent is required or that there is a risk of disproportionate harm to fundamental rights, in particular for children. Data subjects have an unconditional right to object to such processing.

In the CCBE's view, the opt-out mechanism (right to object) that has been created is bound to remain ineffective, as users generally do not know who owns the data contained in a training dataset. Even if they did know, users would have to opt out thousands of times a year, every time another company trains an algorithm with their data. Also, as in case of the proposed changes to Article 9, the proposed provision departs from the principle of technological neutrality.

The CCBE recommends therefore, that the final provision include workable solutions for data subjects to object to the processing of their data, in line with the EDPB and the EDPS who recommended '*clarifying that this right should be brought to the attention of data subjects, when possible and sufficiently in advance of the processing of their personal data, in the context of the development and operation of AI, to enable them to exercise it from the outset*.' In addition, the CCBE recommends that the substantive scope and relationship of the proposed Article 88c GDPR to other provisions be more clearly defined to prevent uncertainty of interpretation. This applies in particular to terms such as 'may be pursued [for legitimate interests within the meaning of Article 6(1)(f) GDPR]', 'where appropriate' or 'enhanced transparency.'

[3] CCBE position paper on the proposal for a regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) (8/10/2021): https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20211008_CCBE-position-paper-on-the-AIA.pdf