December 2025

Digital Omnibus proposal: Suggested Amendments

Despite clear mandates from industry leaders and heads of state, the European Commission's Omnibus proposal fails to address Europe's growing competitiveness gap – it only offers limited adjustments that do not match the scale or urgency of the challenge.

On the AI Act, the Omnibus report does not provide the regulatory certainty or competitive edge Europe needs. Modest improvements—such as expanded legal bases for bias mitigation, more centralized enforcement, and transitional periods—leave core problems intact: disproportionate compliance burdens, legal uncertainty, fragmented timelines, and most fundamentally an innovation-averse framework.

Similarly, for the GDPR and ePrivacy, clarifying legitimate interests for AI development and concepts of personal data and anonymisation in line with CJEU case law are positive but insufficient. The proposal misses the opportunity to firmly embed risk-based proportionality and a clear mandate for regulators to consider innovation and economic impact—reforms that are essential to enable responsible AI development and safeguard Europe's competitiveness.

1. Executive Summary of Recommendations

1.1 AI Act

- **Stop the Clock for the whole AI Act, not just high-risk systems:** The AI Act's upcoming implementation timeline should be paused for the entire framework, including the GPAIM regime, rather than limited to high-risk systems. The current Omnibus proposal - with delayed and staggered high-risk obligations and partial amendments to transparency requirements - creates legal uncertainty for both providers and users. This will allow for a review of the AI Act through other competitiveness initiatives.
    - **We call for:** A coherent pause on the AI Act implementation timeline. High-risk obligations should have a single application date, by amending Article 113(3)(d) so that there is a pause in the application of the high-risk regime until 2 August 2028. The grace period should explicitly extend to GPAIM rules via a new Article 113(b), with Article 101 aligned to the pause of the high-risk regime until 2 August 2028. Article 111(4) should be amended to provide a grace period until 2 February 2028 for all systems under Article 50.
- **Create a regulatory innovation mandate:** The AI Act does not yet provide EU or national regulators with a clear mandate to promote innovation, competitiveness and investment. In the absence of such an innovation mandate, enforcement is likely to remain risk-averse and fragmented, which would slow down the development and deployment of AI within the EU.
    - **We call for:** Introduce Articles 74a and 75a to create a mandate and accountability framework balancing fundamental rights with innovation and economic impact.

- **Maintain broader SCD processing for bias mitigation:** The final Omnibus text rightly broadens the legal basis for processing special category data (SCD) to detect and mitigate bias in all AI systems and models, not only high-risk ones. Limiting bias mitigation to high-risk systems would be fundamentally flawed, as bias is a structural risk that can arise across all AI development.
    - **We call for:** This amendment, introduced in the Omnibus, should be retained in the final text.
- **Reject asymmetric obligations that break the risk-based principle:** Extending reduced penalties and privileges from SMEs to SMCs undermines the core risk-based logic of the AI Act. Risk is determined by the nature of the system and its deployment, not by the size or identity of the provider. Obligations and sanctions should therefore be symmetric for comparable levels of risk, in order to avoid regulatory blind spots, distortions of competition and weakened protection.
    - **We call for:** Revise Article 99(1) to ensure that national rules and penalties do not create asymmetric regulation or unjustified differences in treatment between operators providing equivalent services or comparable activities across Member States.
- **Strengthen central oversight:** Empowering the AI Office as the central supervisor for GPAIMs and for AI used in VLOPs and VLSEs is a welcome step towards consistent enforcement.
    - **We call for:** Support the Omnibus proposal text, with minor clarifications confirming that the AI Office has enforcement powers over all internal AI systems and tools operated by, or on behalf of, such entities, whether used externally or purely internally.

1.2 GDPR & ePrivacy

- **Clarify the definition of personal data:** The Omnibus Proposal rightly links “personal data” to what a controller can reasonably do with the means actually available. However, further clarification is needed to fully reflect CJEU case law and Recital 26 GDPR and prevent fragmented, overly broad interpretations.
    - **We call for:** Retain the Omnibus amendment in the final text, while clarifying that identifiability must be assessed from the perspective of the entity, taking into account also objective factors such as costs, technological resources, time required for identification, and the safeguards applied to the processing.
- **Clarify automated decision-making to prevent over-reach:** The Omnibus clarification that automated decisions are permissible under Article 22, where its conditions are satisfied - even when human decision-making would be possible - constitutes an important step in the right direction.
    - **We call for:** Retain the Omnibus amendment in the final text, while clarifying that Article 22 GDPR applies only to automated decisions that determine a person’s legal status, contractual rights, or have a comparably significant and lasting impact.
- **Harmonising AI and Data Protection:** Article 88c is pivotal, expressly recognising legitimate interest as a legal basis for AI development and operation while aligning GDPR with AI Act concepts. It establishes a clear, EU-wide standard for AI training, reduces legal fragmentation, and effectively modernises GDPR for the AI era.

- **We call for:** Retain the Omnibus amendment, but streamline it to remove ambiguities and overlaps.

- **Amend the concept of joint controllership:** Joint controllership, intended as an exceptional regime for genuine co-determination, has become a de facto general liability framework due to expansive interpretations, now applied broadly and creating legal uncertainty and disproportionate compliance burdens.
  - **We call for:** Targeted amendment to Article 26 clarifying that controllers are to be regarded as joint controllers only where they actively participate in, and actually influence, decisions on the purposes and means of processing.

1.3 Cookies, ePrivacy and Consent

- **Consolidate rules and tackle consent fatigue at the root:** Maintaining a split between GDPR and ePrivacy (GDPR Article 88a vs ePD Article 5(3)) perpetuates complexity, legal fragmentation and consent fatigue, and merely shifting some cookie and tracking rules into the GDPR with limited exemptions fails to address the underlying issues.
  - **We call for:** Repeal ePrivacy Article 5(3) and fully align Article 88a with GDPR legal bases, and place traffic data and direct marketing (i.e. repeal ePrivacy Articles 6, 9, and 13) entirely under the GDPR, without retaining existing ePrivacy provisions.
- **Delete mandatory machine-readable consent signals (Article 88b):** Article 88b would add a new mandatory consent signal layer on top of existing GDPR rules, creating further legal and technical complexity. Past attempts at such signals have failed, and a mandatory scheme would be costly, confusing, especially for SMEs, while exemptions (e.g. for media) would further undermine coherence and user trust.
  - **We call for:** Removing Article 88b in its entirety from the final text.

2. Deep Dive: Proposed Legislative Amendments

2.1 EU AI Act

New Article 4a

SCD for bias detection

Context
The Omnibus proposal introduces a new Article 4a, replacing Article 10(5) AI Act, which provides a lawful way under GDPR for providers and deployers of all AI systems and AI models to exceptionally process SCD for the purpose of ensuring bias detection and correction under certain conditions. This means that, with this proposal, the legal basis for processing SCD to mitigate bias in AI has been broadened to include all AI systems and models, not just high-risk AI systems as

currently stated in the AI Act. This is a positive improvement that will support broader efforts to enable responsible AI training in the EU.

Amendment

Omnibus proposal	**Proposed amendment**
New Article 4a, replacing current 10(5): 1. To the extent necessary to ensure bias detection and correction in relation to high-risk AI systems in accordance with Article 10 (2), points (f) and (g), of this Regulation, providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. In addition to the safeguards set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable, all the following conditions shall be met in order for such processing to occur: /…/ 2. Paragraph 1 may apply to providers and deployers of other AI systems and models and deployers of high-risk AI systems where necessary and proportionate if the processing occurs for the purposes set out therein and provided that the conditions set out under the safeguards set out in this paragraph.	**Support the Current text in Omnibus proposal.**

Justification

The only logical and reasonable approach is for the AI Act to include a clear right to use SCD for bias-mitigation purposes not only in high-risk AI systems but across all AI systems and models. Bias does not arise exclusively in high-risk use cases; it is a structural risk inherent to AI development as such. All models - regardless of their classification as per the AI Act - require the ability to detect, measure, and correct discriminatory patterns, and this cannot be done effectively without access to SCD.

For this reason, extending the bias-mitigation provision beyond high-risk AI to all AI systems and

models is both coherent with the idea of the exemption and highly necessary. It ensures equal standards of fairness, supports responsible innovation, and aligns with the core objective of the AI Act: preventing harm. This is why the proposed approach is logical, proportionate, and should remain in the final Omnibus text.

Article 75: Mutual Assistance, Market Surveillance and Control of General-Purpose AI Systems

Centralized enforcement

Context	
The Digital Omnibus proposal introduces targeted amendments to better align the AI Act with the European Union's broader digital regulatory framework. Notably, the proposed changes to Article 75 seek to expand the enforcement powers of the AI Office, designating it as the central authority responsible for supervising not only GPAIMs and systems developed by GPAIM providers using their own models, but also all AI systems integrated within designated Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLSEs). Given that VLOPs and VLSEs are already subject to exclusive supervision by the European Commission under existing digital regulations, the Commission's amendment addresses potential conflicts between these legislative acts and their enforcement. Furthermore, it harmonizes supervisory responsibilities with the approach established in the DSA, wherein the Commission retains exclusive competence over the largest platforms due to their substantial cross-border impact and the necessity for consistent application of regulatory requirements.	
Amendment	
Omnibus proposal	**Proposed amendment**
Amendment to article 75: "1. Where an AI system is based on a general-purpose AI model, with the exclusion of AI systems related to products covered by the Union harmonisation legislation listed in Annex I, and that model and that system are developed by the same provider, the AI Office shall be exclusively competent for the supervision and enforcement of that system with the obligations of this Regulation in accordance with the tasks and responsibilities assigned by it to market surveillance authorities. The AI Office shall also be exclusively competent	**Support the Current text in Omnibus proposal with minor additions:** "1. Where an AI system is based on a general-purpose AI model, with the exclusion of AI systems related to products covered by the Union harmonisation legislation listed in Annex I, and that model and that system are developed by the same provider, the AI Office shall be exclusively competent for the supervision and enforcement of that system with the obligations of this Regulation in accordance with the tasks and responsibilities assigned by it to market surveillance

for the supervision and enforcement of the obligations under this Regulation in relation to AI systems that constitute or that are integrated into a designated very large online platform or very large online search engine within the meaning of Regulation (EU) 2022/2065."	authorities. The AI Office shall also be exclusively competent for the supervision and enforcement of the obligations under this Regulation in relation to AI systems that constitute or that are integrated into a designated very large online platform or very large online search engine within the meaning of Regulation (EU) 2022/2065, **including all internal AI systems and tools operated by or on behalf of such entities, regardless of whether their use is external or internal in nature**."
Justification	
Centralising enforcement to the AI Office ensures harmonised and coherent oversight of AI systems deployed by Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLSEs), whose operations inherently span the entire internal market. As the EU single market continues to suffer from GDPR enforcement distributed among more than 40 regulators, fragmented national enforcement of the EU AI Act would similarly lead to divergent interpretations and uneven compliance, undermining the integrity of the EU AI single market. The AI Office is better placed to apply a uniform approach and ensure consistent assessments across Member States. A centralised AI Act enforcement—aligned with the DSA's centralised enforcement structure - promotes legal certainty, prevents regulatory fragmentation, and strengthens the EU's capacity to oversee AI in a coordinated and effective manner. However, minor amendments remain essential. Without further clarification, the scope of the legislation is still unclear, and additional uncertainty could arise. To ensure the amendment to this article has its full effect, the legislation must explicitly clarify that the broadened enforcement powers will include all internal AI systems and tools operated by or on behalf of VLOPs and VLSEs, regardless of whether their use is external or internal in nature. This precision is necessary to avoid gaps in oversight and to ensure that the regulatory framework is comprehensive, effective, and future-proof.	

New Article 74a and 75a - Innovation Mandate

Context
The Omnibus proposal confirms a more centralised approach to the AI Act, giving more mandate to the Commission to avoid fragmentation and legal uncertainty. However, it completely fails to

<table>
<tr><td colspan="2">provide a clear mandate for regulators at both EU and national levels to actively promote innovation.</td></tr>
<tr><td colspan="2">Amendment</td></tr>
<tr><td>Omnibus proposal</td><td>Proposed amendment</td></tr>
<tr><td>n/a</td><td>Proposed amended article 74a:
In carrying out their tasks the market surveillance authority shall work to actively promote innovation and economic growth within the Union. This shall include facilitating the development, testing and deployment of artificial intelligence models and systems, disseminating best practices, and fostering cooperation between industry, academia and public bodies. The market surveillance authority shall publish an annual report, including transparent metrics, in order to demonstrate how this objective was integrated in their activities.

Proposed amended article 75a:
In carrying out their tasks the AI Office shall work to actively promote innovation and economic growth within the Union. This shall include facilitating the development, testing and deployment of artificial intelligence models and systems, disseminating best practices, and fostering cooperation between industry, academia and public bodies. The AI Office shall publish an annual report, including transparent metrics, in order to demonstrate how this objective was integrated in their activities.</td></tr>
<tr><td colspan="2">Justification</td></tr>
<tr><td colspan="2">This omission to provide for a clear mandate and an accountability framework for regulators at both EU and national levels to actively promote innovation and economic growth- unaddressed in the Omnibus - prevents the EU to work at the unison in enabling AI to drive societal and economic</td></tr>
</table>

progress. Although the EU AI Act highlights the importance of human-centric and trustworthy AI and the importance of enhancing AI competitiveness and growth, none of these objectives can be achieved if regulatory bodies do not factor economic growth into their activities and are held accountable for. Without a dedicated innovation mandate and accountability parameters, the Act's contribution to EU's global competitiveness in AI development and economic growth at large will be frustrated. Digital regulators must be unified in their mission to create an innovation-friendly and stable environment that advances EU goals for investment, innovation, and sustainable growth. This need was clearly identified by the UK and addressed in its AI Opportunities Action Plan - GOV.UK.

Article 99 - Asymmetric regulation

Context	
In the current omnibus proposal, the EC have included an amendment to article 99, extending existing regulatory privileges on penalties for SMEs to SMCs.	
Amendment	
Omnibus proposal	**Proposed amendment**
New Paragraph 1: 1. In accordance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties and other enforcement measures, which may also include warnings and non- monetary measures, applicable to infringements of this Regulation by operators, and shall take all measures necessary to ensure that they are properly and effectively implemented, thereby taking into account the guidelines issued by the Commission pursuant to Article 96. The penalties provided for shall be effective, proportionate and dissuasive. The Member States shall take into account the interests of SMCs and SMEs, including start-ups, and their economic viability when imposing penalties.	**Proposed amended Paragraph 1:** 1. In accordance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties and other enforcement measures, which may also include warnings and non-monetary measures, applicable to infringements of this Regulation by operators, and shall take all measures necessary to ensure that they are properly and effectively implemented, thereby taking into account the guidelines issued by the Commission pursuant to Article 96. **Member States shall ensure that such rules and measures do not result in asymmetric regulation or unjustified differences in treatment between operators providing equivalent services or engaging in comparable activities across Member States.** The penalties provided for shall be effective, proportionate and dissuasive. ~~**The Member**~~

	~~**States shall take into account the interests of SMCs and SMEs, including start-ups, and their economic viability when imposing penalties.**~~
Justification	
Asymmetric introduction of obligations under the AI Act runs counter to its fundamentals. The AI Act is explicitly designed as a risk-based regulatory framework: obligations scale with the level of risk posed by an AI system, not with the identity or size of the provider. Introducing lighter requirements for certain companies based on company size not only violates this core principle but also results in unfair discrimination. Risk is inherent in the system, not in the size of its developer. A high-risk AI system can be created by a startup just as easily as by a large corporation. Large corporations can neither be equated to a "high-risk" by default approach. The potential for harm results from how an AI system actually functions and where it is deployed. Using company size as a proxy for risk is a discriminatory measure that misrepresents the structure and intent of the Act, and creates regulatory blind spots precisely where safeguards are needed most. For the AI Act to remain coherent, effective, and faithful to its foundational logic, obligations must apply symmetrically to all actors developing or deploying systems of comparable risk. Departures from this principle dilute protections for citizens and create an uneven market, compromising both safety and competitiveness in the Union.	

Article 111 (referring to Article 50(2)) - Stop-the-Clock for Watermarking Obligations

Context
In the final omnibus package, the European Commission is proposing a grace period for certain transparency requirements to ensure that providers of generative AI systems have sufficient time to adapt their practices without causing market disruption. Specifically, the Commission recommends a transitional period of six months for compliance with Article 50(2). To implement this, the Commission proposes amending Article 111(b) to include the following provision: "Providers of AI systems, including general-purpose AI systems generating synthetic audio, image, video, or text content, that have been placed on the market before 2 August 2026 shall take the necessary steps to comply with Article 50(2) by 2 February 2027." The grace period means that AI systems which generate synthetic content and **were already available before 2 August 2026** have extra time to follow the new transparency rules. These

providers must comply by 2 February 2027 at the latest. In other words, **existing systems get a transition period** to adjust, but after that date, they must meet the new requirements.

Amendment	
Omnibus proposal	**Proposed amendment**
New Paragraph 4: 4. Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, that have been placed on the market before 2 August 2026 shall take the necessary steps in order to comply with Article 50(2) by 2 February 2027.'	**Proposed amended Paragraph 4:** 4. Providers of AI systems ~~**including general-purpose AI systems, generating synthetic audio, image, video or text content, that have been placed on the market before 2 August 2026**~~ shall take the necessary steps in order to comply with ~~**Article 50(2) by 2 February 2027**~~ **Article 50 by 2 February 2028.**

Justification
The proposed grace period for Article 50.2 should instead be extended to cover all of Article 50. Limiting the grace period to specific sections, as well as limiting the grace period only to AI systems placed on the market before August 2026, is unjustified. The same technical and practical challenges apply across all provisions, and the need for clarification and readiness for enforcement is universal. The grace period must apply to all AI systems in scope of the transparency requirements in article 50, regardless of their market entry date, with a unified pause until February 2027. This is essential, as there is currently no consensus on the Code for labelling and watermarking. Restricting the grace period both to just one section of article 50, as well as to AI systems released before a certain date, undermines predictability and risks stifling innovation. The Commission should ensure the grace period applies to Article 50 in its entirety, at least Articles 50.1–50.6, to achieve the intended and urgently needed effect. Furthermore, the implementation grace period should be extended to 2 August 2028, aligned with a pause on implementation applicable to the rest of the AI Act, including both high-risk systems and GPAI models.

Article 113 and Annex III - Stop-the-Clock for High-Risk Systems

Context

The final Omnibus report on the AI Act sets a grace period for high-risk AI systems, which begins once the Commission confirms that supporting measures (e.g., standards or guidelines) are in place. If not confirmed in time, the rules will automatically apply by the final deadline.

- Earliest possible start:
  - 6 months after Commission confirmation (Annex III systems)
  - 12 months after Commission confirmation (Annex I systems)
- Latest possible start:
  - 2 December 2027 (Annex III systems)
  - 2 August 2028 (Annex I systems)

While the flexible timeline creates some uncertainty, it is likely that the regulations will take effect in August 2027. CEN-CENELEC plans to finalize high-risk standards by Q4 2026, leaving about six months until the final deadline. However, this may change if the Commission accelerates the process.

Amendments

Omnibus proposal	**Proposed amendment**
In the third paragraph, point (d) is added: (d) Chapter III, Sections 1, 2, and 3, shall apply following the adoption of a decision of the Commission confirming that adequate measures in support of compliance with Chapter III are available, from the following dates: (i) 6 months after the adoption of that decision as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and (ii) 12 months after the adoption of the decision as regards AI systems classified as high-risk pursuant to Article 6(1) and Annex I. In the absence of the adoption of the decision within the meaning of subparagraph 1, or where the dates below are earlier than those that follow the adoption of that decision, Chapter III, Sections 1, 2, and 3, shall apply: (i) on 2 December 2027 as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and (ii) on 2 August 2028 as regards AI	**Proposed new third paragraph, point (d):** The provisions of this Regulation relating to high-risk AI systems, as set out in Annex I and Annex III, shall apply from August 2, 2028.

systems classified as high-risk pursuant to Article 6(1) and Annex I.	

Justification

The current suggested amendment to the AIA introduces multiple, conditional timelines based on Commission confirmation of supporting measures, resulting in significant legal uncertainty for both businesses and member state regulators. It is unclear what would trigger a Commission decision, and the possibility of different start dates for different systems (Annex I vs. Annex III) further complicates compliance planning.

The EC should replace the current staggered and conditional grace period for high-risk AI systems with a single, comprehensive pause clarifying that all provisions relating to high-risk AI systems (Annex I and Annex III) shall take effect on a specific date. This would ensure:

- Legal certainty: Businesses and regulators understand that compliance deadlines are on hold based on a clear, predictable timeline.
- Administrative simplicity: Avoids confusion and reduces the risk of misinterpretation or inconsistent application across member states.

The proposed grace period is insufficient and uncertain, and should be extended to 2 August 2028 and aligned with a pause on implementation for the rest of the AI Act, including transparency rules and GPAI models.

Article 113 - Stop-the-Clock for GPAIM

Context

Article 113 of the AI Act sets out the entry into force and application timelines for its various provisions and chapters. The final Digital Omnibus proposes amendments to Article 113, specifically paragraph three, points (d) and (e).

In accordance with relevant EU case law - most notably C-65/93 Parliament v Council - co-legislators may introduce further amendments, provided these do not alter the essential purpose of the proposal or exceed its legal basis. As such, while amendments introducing substantial new policy are out of scope, it remains permissible to adjust the timeline for the General Purpose AI Models (GPAIM) regime within the AI Act through the omnibus, since Article 113 is already being revised to address implementation timelines.

Amendments

Omnibus proposal	**Proposed amendment**
n/a	**Proposed new point (b) to Article 113:** (b) Chapter III Section 4, Chapter V, Chapter VII

	and Chapter XII and Article 78 shall apply from 2 August 2025, with the exception of Article 101, which shall apply from 2 Aug 2028.

Justification

Postponing only the High-Risk regime in the AI Act acknowledges implementation pressures, but does not resolve the broader compliance burden, ongoing lack of legal certainty for businesses operating in the EU or impact on EU innovation overall. These challenges are not limited to High-Risk systems; they also affect the provisions for GPAIM, as the GPAIM rules blur the distinction between model development and system use. This approach diverges from the established principle that risk should be managed where it materializes - in the use of AI systems.

By pausing only the High-Risk regime and not the GPAIM rules, the legislative process risks falling short at the final stage and missing its goal of comprehensive, effective regulation. Extending the postponement to GPAIM provisions is essential for legal certainty and for maintaining a truly risk-based approach.

Moreover, the current GPAIM framework conflates the development of AI models with the deployment and use of AI systems, undermining effective risk management and threatening the stability of the regulatory framework. This is why the Digital Omnibus and other competitiveness initiatives must undertake a broader and more comprehensive review of Article 113, as well as the referenced Article 101, to ensure consistency. Only through such decisive action can the AI Act deliver its intended results without stifling innovation or hindering the development and deployment of transformative AI technologies in the EU. As such, the Omnibus should introduce a grace period for the GPAIM regime until 2 August 2028, in line with the pause on implementation for the rest of the AI Act, including transparency rules and High-Risk systems.

2.2 GDPR

Article 4(1) - Personal Data Definition

Context

The Commission's Omnibus proposal amends Article 4(1) GDPR to codify the CJEU's jurisprudence (SRB, Breyer) on identifiability, confirming a relative concept of anonymisation. This means information is personal data only if a person or entity is reasonably likely to identify the individual using realistically available means, moving away from the broad, absolute interpretation often adopted by the EDPS and DPAs. Such expansive views have led to inconsistent enforcement,

disproportionate compliance burdens, uncertainty for innovative services and AI, low legal predictability for SMEs, and deviations from GDPR's original intent. The Commission's text provides a needed shift towards a practical, risk-based understanding of identifiability.

Amendment	
Omnibus proposal	**Proposed amendedment**
Amendments to Article 4(1): 'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'	**Support the Current text in Omnibus proposal with small additions.** 'Information relating to a natural person is not necessarily personal data for a person or entity. Information shall not be personal for a given entity where that entity is not reasonably able to identify the natural person to whom the information relates, taking into account the means reasonably likely to be used **in practice by that entity, considering all objective factors, such as the costs, technological resources and the amount of time required for identification and the safeguards applied to the processing.** Such information does not become personal for that entity merely because **the entity which sent the data to that entity or a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'**

Justification
Embedding CJEU Doctrine for Legal Certainty and Harmonisation The Commission's proposal codifies the CJEU's SRB and Scania rulings, clarifying that identifiability depends on whether a specific entity has means reasonably likely to be used to identify an individual. The amendment further defines "reasonably likely" by referencing practical factors—time, cost, technology, and safeguards. This statutory language translates case law into clear operational criteria, ensuring consistent interpretation, reducing regulatory overreach, and

harmonising enforcement across Member States. It addresses fragmentation from divergent DPA interpretations and establishes a stable baseline for application.

Proportional, Risk-Based Scope with Strong Protection
By requiring identifiability to be assessed from the entity's perspective, the amendment prevents regulatory overreach and upholds the GDPR's protection standard. It responds to concerns about DPAs and the EDPB adopting overly broad definitions, ensuring GDPR applies only when identification is genuinely plausible. This risk-based approach aligns with Recital 26 and Article 4(1), incentivises safeguards like encryption and pseudonymisation, and preserves meaningful privacy protection without unnecessarily expanding the Regulation's scope.

In Conjunction with Article 41a: Innovation, Consistency, and Future-Proofing
Together with Article 41a, these clarifications ensure future rules on pseudonymisation and anonymisation are based on harmonised criteria. The proposal delivers a future-proof, proportionate, and coherent framework that simplifies regulation, supports EU digital competitiveness, and maintains robust data protection.

Article 22 - Automated Decision-making

Context
The Digital Omnibus seeks uniform interpretation, legal certainty, and simplification that enable EU AI goals and EU competitiveness goals to become a reality. The EC's clarification on automated decision-making in Art. 22 GDPR, confirming that automated decisions are permissible when conditions are met, even if human decision-making is possible, is positive improvement. Additionally, it is important to note that Article 22 GDPR uses the terms "legal effects" and "similarly significantly affects," but does not define them. As a result, extreme interpretations by data protection supervisory authorities equating any algorithm to an automated decision that has legal effects (such as the recent draft EDPB Guidelines on DSA/GDPR) or construing the right to challenge this kind of automated decisions and ask for human intervention to a prohibition that has never existed in the GDPR nor in its predecessor (the Directive 95/46/EC)—have broadened the provision beyond what the legislator intended and beyond the threshold confirmed by the Court of Justice in C-634/21 (SCHUFA), making impossible the development of any processing where AI is involved. The Digital Omnibus seeks uniform interpretation, legal certainty, and simplification that enable EU AI goals and EU competitiveness goals to become a reality. An additional short clarifying

<table>
<tr><td colspan="2">sentence would ensure Article 22 is applied consistently and proportionately and corrects the above-mentioned overreach.</td></tr>
<tr><td colspan="2">Amendment</td></tr>
<tr><td>Omnibus proposal</td><td>Proposed amendedment</td></tr>
<tr><td>Amended Article 22, paragraphs 1 and 2:
1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data
subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent.’

2. n/a</td><td>Support the Current text in Omnibus proposal, with an additional paragraph 2.
1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data
subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent.
2. For the purposes of paragraph (1), legal effects arise only where the decision decisively determines a data subject’s legal status, their legal entitlement, or their rights under a contract; and similarly significant effects arise only where the decision is comparable in significance to a legal effect and has a prolonged or permanent impact on a data subject that may lead to their systemic exclusion, them incurring significant financial consequences, or inhibiting their access to essential services.</td></tr>
<tr><td colspan="2">Justification</td></tr>
</table>

Legal Certainty and Alignment with CJEU Case Law

The amendment codifies the CJEU's interpretation that Article 22 GDPR applies only to automated decisions that determine a person's legal status, contractual rights, or have a comparably significant and lasting impact (e.g., access to social benefits, admission or residence rights, contract cancellation, or decisions resulting in exclusion or discrimination). By setting this high threshold in law, it ensures consistent application across the EU, enhances legal certainty, and preserves the protective intent of Article 22 without changing its substance, thereby reducing divergent national interpretations.

Proportionate Scope and Correction of Overreach

The amendment confirms that Article 22 is limited to decisions with genuine, prolonged, or permanent effects, avoiding the unintended inclusion of routine, low-impact automated processes (such as fraud alerts or preliminary risk assessments subject to human review). This proportionate approach maintains strong safeguards for high-risk decisions while reducing unnecessary compliance burdens and correcting overly expansive supervisory guidance, in line with the GDPR's risk-based design.

Enabling Innovation and Global Competitiveness

By clarifying when Article 22 applies, the amendment offers predictable rules for the deployment of AI and automated systems. Public and private actors can scale beneficial automation—such as compliance tools, fraud detection, and administrative workflows—without undue legal uncertainty. This clarity supports innovation and digital transformation in the EU while upholding high standards of fundamental rights protection in genuinely consequential decisions.

Article 26 - Joint Controllership

Context

Joint controllership under GDPR Article 26 was originally conceived as an exceptional regime, intended only for situations involving genuine co-determination of purposes and means between parties. However, over time, a series of CJEU rulings - including Wirtschaftsakademie, Fashion ID, Jehovan todistajat, IAB Europe, and Russmedia have been broadly misunderstood and resulted in legal uncertainty. Along with that, expansive interpretations by national Data Protection Authorities (notably the German BfDI), have significantly broadened the application of Article 26. What was meant to be a narrowly tailored provision has evolved into a general liability framework, now applied to a wide range of relationships and technical integrations that go far beyond the legislature's original intent.

This shift has far-reaching consequences for all types of entities, regardless of sector or size - affecting both offline and online activities, and impacting commercial enterprises, public institutions, and SMEs alike. The resulting legal uncertainty and compliance burden underscore

<table>
<tr><td colspan="2">the need for clarification and recalibration of the joint controllership regime to restore its original, limited purpose and to support a more predictable and proportionate application of the GDPR.</td></tr>
<tr><td colspan="2">Amendment</td></tr>
<tr><td>Current text in Omnibus proposal</td><td>Proposed amendedment</td></tr>
<tr><td>n/a

Original GDPR language:

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.</td><td>Proposed clarification on Art.26:

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. Controllers shall be considered to jointly determine the purposes and means of processing, only if they actively participate in and actually influence decisions on the purpose and means of processing. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.</td></tr>
</table>

Justification	
Legal and Policy Justification CJEU decisions—from Wirtschaftsakademie to Russmedia—have expanded joint controllership well beyond the GDPR's original intent. Courts now find joint responsibility even where entities lack access to data or influence over processing, creating a structural mismatch with Article 4(7) and the single-accountability logic of Articles 5(2) and 24. The Digital Omnibus and Digital Fitness Check both identify legal uncertainty, regulatory overlap, and unnecessary complexity as critical issues. Article 26, shaped by unpredictable jurisprudence, exemplifies the inconsistency the Omnibus seeks to eliminate for a simpler, more coherent regulatory framework. **Operational and Economic Justification** The broad joint-controller doctrine, as interpreted by the CJEU, forces entities—including SMEs and public institutions—to maintain complex Article 26 arrangements for even minimal interactions. This leads to unclear responsibilities, duplicated transparency notices, unnecessary DPIAs, lengthy contractual negotiations, and disproportionate liability. National DPAs, such as the BfDI, have further expanded the scope, treating common website integrations as joint controllership and causing regulatory fragmentation. Clarifying Article 26 would immediately reduce compliance burdens and support a more accessible, innovation-friendly environment. **Enforcement and Future-Proofing Justification** Joint controllership complicates DPA enforcement, requiring authorities to apportion responsibility—often inconsistently across Member States. This undermines coherence, predictability, and user understanding. The Omnibus aims for harmonised EU enforcement and consistent digital rules. Clarifying Article 26 would remove a major source of divergence and deliver the clarity and uniformity needed for a future-proof regulatory landscape. A clarified joint-controller rule will provide for much needed legal certainty for controllers, DPAs, and individuals alike.	

Article 88(c) - LI for AI development

Context
The European Commission suggests the very welcomed new Article 88c to the GDPR to clarify how personal data may be used for developing and operating AI under the GDPR. Although the EDPB's Opinion on AI Model Training has confirmed that legitimate interest may serve as a lawful basis for AI training, the guidance leaves considerable scope for interpretation by individual DPAs. This creates a risk of inconsistent application across Member States.

Furthermore, the adoption of the AI Act has introduced a new regulatory framework and new definitions - such as AI systems, AI models, and General Purpose AI (GPAI) - which must be harmonized with the GDPR's requirements for lawful processing. Alignment between these frameworks is essential to ensure legal certainty and consistent enforcement throughout the EU.

The rapid growth of AI exposed gaps in the GDPR's original wording, especially regarding large-scale data ingestion, model training, residual memorisation risks, and transparency obligations. Article 88c responds to these issues by giving explicit legal recognition to the use of legitimate interests for AI development, while linking GDPR obligations directly to the AI Act's structure and terminology.

Amendment	
Omnibus proposal	**Proposed amendedment**
New Article 88c: Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data	**Proposed amended Article 88c:** Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union ~~**or national**~~ laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data~~**, in particular where the data subject is a child.**~~ Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject~~**, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an**~~

subjects with an unconditional right to object to the processing of their personal data."	~~**unconditional right to object to the processing of their personal data.**~~"

Justification

Article 88c introduces a unified, EU-wide legal framework for processing personal data in AI development, ensuring legal certainty and harmonisation. By incorporating EDPB principles into the GDPR, it transforms guidance into binding law, providing organisations with a stable compliance foundation. This update modernises the GDPR for the AI era, aligns it with the AI Act, and clarifies the use of legitimate interest for AI training, balancing innovation with the protection of fundamental rights.

However, the draft currently contains unnecessary ambiguities and overlapping requirements, which could undermine clarity. Streamlining these elements would further strengthen the regulation's effectiveness. For instance, including "national laws" as an exception undermines GDPR harmonization and risks regulatory fragmentation. Furthermore, referencing children is unnecessary, as the GDPR already requires special consideration for vulnerable groups in the balancing test. Specifying safeguards in the legal text restricts flexibility and may stifle innovation; the GDPR's existing requirements for appropriate measures are sufficient.

2.3 ePrivacy and GDPR Consolidation

Article 5(3) ePD and 88(a) GDPR - Terminal equipment ("Cookies") rule

Context

The Commission's Omnibus Proposal introduces Article 88a GDPR, which creates a new, consent-focused regime for accessing and storing information on users' devices. This provision closely follows and expands the logic of Article 5(3) of the ePrivacy Directive ("cookies clause"), making consent the default legal basis and allowing only four narrowly defined exemptions. Article 88a also imposes strict user interface requirements, such as mandatory single-click consent and a six-month "no re-ask" period, which apply to both initial and subsequent data processing.

This approach is highly restrictive, essentially reinstating a consent-centric cookie regime within the GDPR and leaving little room for legitimate interests or other legal bases under Article 6(1). It departs from the GDPR's established risk-based system and the flexible consent conditions of Article 7. While the Commission aims for simplification and coherence, Article 88a instead creates

a complex sub-regime, introducing new technical requirements and consent infrastructure that add to the existing GDPR and ePrivacy frameworks, increasing complexity and legal uncertainty.

The exemptions, especially for first-party measurement (limited to processing "for the sole benefit of the controller"), are too narrow to be practical for most SMEs and measurement vendors, and do not reflect a risk-based, proportionate approach. The prescriptive UI rules further limit flexibility and innovation in consent management, making it difficult for smaller publishers and advertisers to process cookie data, even with consent. This results in a disproportionate compliance burden, greater risk of GDPR fines, inconsistent enforcement, and increased user consent fatigue. Creating a parallel rule for terminal equipment is therefore redundant and counterproductive, destabilising the legal framework and undermining the Omnibus Proposal's stated objectives.

Amendment	
Omnibus proposal	**Proposed amendedment**
New Art. 88a: (1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation. (2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1). (3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following: (a) carrying out the transmission of an electronic communication over an electronic communications network;	**Proposed amended Article 88a:** (1) This Article applies where the storage of information in the terminal equipment of a data subject or the access to information already stored in that equipment constitutes the processing of personal data. (2) Such processing shall be lawful only if and to the extent that at least one of the legal grounds set out in Article 6(1) apply. For the purposes of this paragraph, the storing of personal data, or gaining access to personal data already stored, in the terminal equipment of a data subject and subsequent processing, shall be lawful to the extent it is necessary for any of the following: (a) carrying out the transmission of an electronic communication over an electronic communications network may be necessary for the performance of a contract within the meaning of Article 6(1)(b) of Regulation (EU) 2016/679; (b) providing a service explicitly requested by the data subject may be necessary for the performance of a contract within the meaning of Article 6(1)(b) of Regulation (EU) 2016/679;

(b) providing a service explicitly requested by the data subject; (c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use; (d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service. (4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply: (a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means; (b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject; (c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months. This paragraph also applies to the subsequent processing of personal data based on consent. (5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]	(c) the interests of the controller in the context of measurement and analytics, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject; and (d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service may be necessary for the performance of a contract within the meaning of Article 6(1)(b) of Regulation (EU) 2016/679.

After Article 5(3), the following subparagraph is added: 'This paragraph shall not apply if the subscriber or user is a natural person, and the information stored or accessed constitutes or leads to the processing of personal data.'	**Proposed deletion of Article 5(3) in conjunction with Proposed amended Article 88a** Fall back in case proposed amendment to 88a is not adopted: *Support 5(3) subject to minor amendment:* After Article 5(3), the following subparagraph is added: 'This paragraph shall not apply if the subscriber or user is a natural person, and the information stored or accessed constitutes the processing of personal data.'
Justification	
Legal and Regulatory Coherence Amending the Omnibus Proposal to delete Article 5(3) of the ePrivacy Directive and revise Article 88a to fully align with the GDPR would restore legal and regulatory coherence. The GDPR already offers a comprehensive, risk-based framework for all personal data processing, including activities involving terminal equipment. Relying on the GDPR's established legal bases—such as legitimate interests and contractual necessity—avoids duplicative and conflicting requirements, eliminates confusion from parallel regimes, and provides clear, predictable rules for all stakeholders. This supports the Commission's goals of simplification and coherence. **Proportionality, User Experience, and Innovation** Allowing all GDPR legal bases for terminal equipment processing ensures a proportionate approach that reflects the actual risk and context of each activity. It reduces unnecessary reliance on consent banners, which have led to user fatigue and weakened the effectiveness of consent as a safeguard. Legitimate interests and contractual necessity enable essential, low-risk processing—such as analytics, fraud prevention, and user experience improvements—without unnecessary barriers, while maintaining transparency and respect for user rights. This fosters innovation and flexibility for data-driven business models, ensuring privacy protections remain robust and user-centric. **Supporting SMEs and Reducing Compliance Burden** A GDPR-aligned approach is especially important for SMEs and smaller publishers or advertisers, who are disproportionately affected by complex, consent-first regimes and the risk of higher fines.	

Removing redundant rules and relying on GDPR principles like data minimisation and privacy by design reduces compliance costs and levels the playing field. This strengthens privacy protections and supports a competitive, innovative digital economy, in line with the Commission's objectives. In summary, deleting Article 5(3) and revising Article 88a to fully integrate with the GDPR is the most effective way to achieve legal certainty, regulatory simplicity, and sustainable privacy outcomes for all stakeholders.

Article 88(b) - Automated choice

Context	
The Commission's Omnibus Proposal introduces Article 88b GDPR, which would require browsers, operating systems, apps, and intermediaries to implement technical frameworks for transmitting machine-readable consent signals. Controllers would be obligated to detect and interpret these signals, while certain media providers may be exempt. Additionally, a new "trusted flagging infrastructure" would be added to existing consent mechanisms. This proposal creates a parallel consent-management regime within the GDPR, separate from the established consent conditions in Article 7, the legal bases in Article 6, and the ePrivacy framework. This approach contradicts the Omnibus Proposal's stated goals of streamlining digital regulation, reducing complexity, easing burdens on SMEs, simplifying rules for controllers and DPAs, and focusing on risk rather than formality. Experience shows that top-down, EU-wide consent tool mandates have repeatedly failed. The EU Cookie Pledge faced strong industry resistance and was abandoned. Efforts to require browser-level consent settings under the ePrivacy Regulation have been stalled for nearly a decade due to political and technical challenges. The German PIMS model has seen only limited, voluntary adoption, hindered by technical complexity. In light of this history, a mandatory, infrastructure-level consent signal rule appears unrealistic and misaligned with the Omnibus Proposal's core objectives.	
Amendment	
Omnibus proposal	**Proposed amendedment**
New Art. 88b: Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons	**Propose deletion of Article 88b.**

(1) Controllers shall ensure that their online interfaces allow data subjects to: (a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled; (b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means. (2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1. (3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service. (4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices. Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1. (5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation]. (6) Providers of web browsers, which are not	

SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article. (7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].	

Justification

The GDPR already offers a comprehensive framework for consent management through Articles 6, 7, and 12–14. Introducing a separate, mandatory consent regime—such as browser or OS-level signals—would create duplicative and potentially conflicting systems, undermining legal clarity, legal certainty and user autonomy. This risks confusion over what constitutes valid consent, including how consent at the level of terminal equipment access interacts with consent or other legal bases for subsequent data use under Article 6 GDPR; incompatibility with existing standards, and increased litigation.

No interoperable technical standard exists for universal, machine-readable consent signals across browsers, operating systems, apps, and devices. Previous attempts, like the Cookie Pledge and ePrivacy browser mandates, have failed due to political and technical challenges. Imposing such requirements would disproportionately burden SMEs, forcing them to implement complex systems and legal vetting, while larger organisations are better equipped to adapt. In practice, mandatory browser or OS-level privacy controls operating at the point of access to or storage on terminal equipment (e.g. cookie consent tools) risk de facto constraining or invalidating reliance on Article 6 GDPR for data use, not just data collection, by creating a separate authorisation layer that controllers must align with their purpose-based legal basis assessment.

Mandatory browser or OS-level privacy controls have proven politically unworkable, contributing to legislative deadlock and regulatory fragmentation. Exemptions for media services further undermine user trust and equal treatment. Rather than enhancing privacy, a second consent regime would fragment protections, confuse users, and weaken the effectiveness of the GDPR. Under the GDPR, the purposes and conditions of data processing should drive the choice of legal basis and should cover, in a coherent and transparent way, both the collection of data (including any access to terminal equipment) and its subsequent use for clearly defined purposes.

Delete Articles 6,9 and 13 - Direct Marketing and Traffic Data

Context	
The Digital Omnibus proposal already migrates Article 5(3) ePrivacy into the GDPR (Article 88a), but leaves key personal data processing rules fragmented across multiple frameworks. Direct marketing and traffic metadata remain split between GDPR and ePrivacy, so OTT messaging providers, telecom operators, and digital advertising businesses must operate under dual regimes. At the same time, 27 Member States maintain divergent implementations—such as varying soft opt-in rules, national telecom secrecy provisions, and inconsistent traffic-data principles—while the outdated 2002 ePrivacy Directive continues to coexist with the modern GDPR. This partial consolidation produces an incoherent regulatory architecture, separate from the comprehensive personal data framework and unified legal basis system under Article 6 GDPR, and at odds with the streamlined approach promised by the Omnibus reform. The Commission itself frames the Omnibus as an effort to "streamline the digital acquis," "reduce unnecessary complexity and burden on SMEs," and "simplify rules for controllers and DPAs" to promote coherence in the digital single market, yet the current design preserves precisely the kind of fragmentation it seeks to remove. Experience shows that maintaining parallel GDPR and ePrivacy regimes generates persistent compliance challenges: cross-border inconsistencies in direct marketing and traffic data rules; dual compliance burdens for controllers; a technological mismatch between a 2002-era framework and today's converged communications ecosystem; and regulatory uncertainty caused by overlapping data protection and telecom oversight. Against this background, completing the consolidation of personal data rules within the GDPR framework is both logical and necessary.	
Amendment	
Omnibus proposal	**Proposed amendedment**
n/a	**Proposed amendments to Directive 2002/58/EC** ● Delete Article 13 ● Delete Articles 6 and 9 (insofar as they concern the processing of personal data).
Justification	
The GDPR already governs direct marketing and communications metadata as personal data, through Articles 6, 7, 12–14, and 21. Existing ePrivacy rules largely duplicate and sometimes	

conflict with these provisions, adding complexity without strengthening protection. Consolidating these areas into GDPR adds no new obligations; it simply relocates existing rights into a coherent framework, supported by two modern, minimal definitions (direct marketing communication; traffic data) rather than outdated telecom concepts.

This consolidation removes the dual compliance burden of applying GDPR alongside 27 variants of ePrivacy Article 13 and divergent traffic-data regimes for telecoms and OTTs. Under a GDPR-only model, controllers follow a single transparency regime, one legal-basis system, one objection right, one retention framework, and one enforcement mechanism via the GDPR consistency system. This aligns fully with the Omnibus objective to streamline the digital acquis, reduce fragmentation and administrative burden - particularly for SMEs - strengthen technological neutrality ("same activities, same risks, same rules"), and avoid reopening politically toxic ePrivacy negotiations.

A unified GDPR framework supports innovation and fair competition by applying equivalent rules to telecoms and OTTs, and by providing consistent governance for traffic metadata used in AI development, fraud detection, cybersecurity, and network integrity. Users benefit from clearer, harmonised rights (including objection and transparency), and high-risk metadata processing becomes subject to DPIAs. Completing this reform finally removes the last 2002-era personal-data enclave, delivering a modern, harmonised, and competition-neutral regime that is legally coherent, economically rational, and fully in line with co-legislators' priorities.