IPoP's Position Paper – Digital Omnibus

Margo Bernelin, Nataliia Bielova, Pierre Bourhis, Juliette Sénéchal, Ludovica Robustelli, William Letrone, Julien Rossi, Jonathan Keller, Pierre Laperdrix, Lionel Seinturier

IPoP's Position Paper – Digital Omnibus

March 2026

This position paper has been prepared for the Commission's call for evidence on the Proposal for *a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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 (Digital Omnibus).*

Interdisciplinary Project on Privacy - IPoP

IPoP is a French interdisciplinary research project that focuses on new forms of personal information collection, on the learning of Artificial Intelligence (AI) models that preserve the confidentiality of personal information used, on data anonymisation techniques, on securing personal data management systems, on differential privacy, on personal data legal protection and compliance, and all the associated societal, legal and ethical considerations. This unifying interdisciplinary research program brings together internationally recognised research teams (from universities, engineering schools and institutions) working on privacy.

Contributors (alphabetical order): Nataliia Beliova, Margo Bernelin, Pierre Bourhis, Jonathan Keller, Pierre Laperdrix, William Letrône, Ludovica Robustelli, Julien Rossi, Lionel Seinturier, Juliette Sénéchal.

Introduction:

Our general appraisal of the Digital Omnibus is that the envisioned reform will have significant negative consequences for data protection. We are concerned that the modifications will not benefit the data subject nor will it offer a real simplification for data processors.

To express our analysis, we opted for a synthetic document targeting specific elements including definition issues (personal data ; scientific research), data subjects' rights, cybersecurity issues, personal data processing for AI systems, scope of user agent's mediated consent.

Outline:

Definition of personal data

Art.3 pt1 and recital 27 of the proposed Digital Omnibus Regulation substantially modify the definition of personal data. The new definition **is not aligned with the current legal landscape**:

- It does not quite translate the CJEU's SRB decision (C-413/23 EDPS v SRB, pt.85), nor the Court's case law on personal data (IAB Europe C-604/22 pt. 46; Scania case C-251/22 pt 49; Nowak, C-434/16);
- It goes against article 8 of the Charter of Fundamental Rights (which has the same legal force as the treaties) which is based on the definition of personal data under Directive 95/46;
- It also disregards the fact that the GDPR applies to the processing of personal data, and not to entities holding or in possession of such data[1]. Whenever personal data is processed, rights and duties are attributed to data subjects and data controllers.

Moreover, the definition lacks **clarity on what is targeted as an "entity"**, is it the controller, joint controller or processor?
For those reasons, if kept intact, the new definition will create **practical difficulties**, especially for business build upon data transfer such as **data brokers**. It could also create complexity in for the **controller-processor relationship** if, under the new definition, one is no longer subjected to the GDPR (art. 32 and 28.10 GDPR being examples of application difficulties).
Practical difficulties are also foreseen for sector-specific applications where sensitive data are processed (e.g. **health**), and for which lowering the level of data protection will be problematic. Indeed, by considering that, in some case, pseudonymised data are anonymous, sensitive data's protection will be jeopardised as, in this scenario, the data will not be considered personal, and therefore the obligation to technically protect them (art. 24 and 32 GDPR) will no longer apply. It will have consequences over Health Data Regulation in Member States as well as for the European Health Data Space Regulation 2025.

Problems could also arise in the event of **international transfers**: if the EU repealed its Personal Data Protection legislation, then other countries that adopted their legislation based on the GDPR could refuse to transfer personal data to the EU, judging that the European's level of protection is lower than theirs.

Finally, under Article 41(a), the **Commission** hints at the possibility of **determining whether pseudonymisation techniques render the data anonymous**. This is the **role of the legislator, which contradicts with the principle of institutional balance in the EU**. Furthermore, this article envisages that the Commission would do this using implementing acts adopted under the procedure set forth in Article 93 (3) GDPR, that is to say, an emergency procedure under the EU's rules on comitology.

Definition of "research purposes"

The inscription of the definition of research purposes within art. 4 of the GDPR is aimed at boosting data processing for economic development, including the development of AI systems. As a consequence, its **articulation with more protective disposition such as the principle of data minimisation is unclear**. This new definition should also be read in light of Article 13.5

[1] See EUCJ 5 Dec. 2023, C-683/21, *NVSC*.

(Article 3(6)), which lightens the information obligations whenever data are used for research purposes by making them publicly available. The outcome is lower protection for the data subject.
The consequences of the new definition of scientific research should be investigated further in light **of how all these provisions interact with each other and the effects this has on other regulations**. The definition will also have an impact on other text, such as the European Health Data Space Regulation that aims at health data, which are sensitive by nature and to their processing based on the *legitimate interest* legal basis.

In addition, **the reference to ethical standards is not enforceable**, as there are no agreed standards in the economic research area.

Academic research not aimed at innovation could be excluded from the definition.

The processing of sensitive data for AI development

The addition of Art. 9(2)(k)(l) and §5 (Art. 3, pt. 3) means that sensitive data can be used for **AI development**. This extends the exception already allowed under Article 10.5 AI Act when it comes to bias correction. Such extension, will lower data protection standards and seems contrary to the proportionality principle in art. 52.1 of the Charter. **Broadening the use to sensitive data is particularly problematic in light of data leakage and hallucinations associated with the use of generative AI.**

Within this proposal, the use of **biometric data** for authentication is permitted when the user is the sole person with access to the data. However, this case scenario seems very limited, as a lot of devices do not limit data access to the user, hence questioning the relevancy of this addition.

Data subjects' rights

The Digital Omnibus contains proposals to limit some of the rights of data subjects. The right of access would be the most affected, under Article 3 (5), amending Article 12 (5) of the GDPR. It aims, among other things, at limiting **the right of access** to cases where the request is made for "data protection purposes". Such purposes can be quite extensive. They cover checking the lawfulness of a processing operation and supporting any right supported by the data protection. But they are also a **vague and confusing formulation, which creates uncertainty and a high risk of litigation that is costly both for data subjects and data controllers, whereas, at the same time, the GDPR is already equipped with provisions that allow controllers to refuse excessive requests.** Aligning with conclusions drawn from other research projects we would advise against the proposed changes in Article 3 (5) of the Digital Omnibus.

Cybersecurity incident notification

Article 3 (8) of the Digital Omnibus proposes tasking **ENISA** with managing a single point of contact to notify data violations and other cybersecurity incidents. This creates simplification of notification duties where there is significant overlap between the GDPR and security legislation, such as NIS2. The 24 additional hours granted to data controllers are not a major change. However, one major change is **that data controllers will now only be required to notify data breaches, when they deem them as presenting "a high risk to the rights and freedoms of natural persons**", as a rule, whereas now, under Article 33 of the GDPR, data controllers could avoid notification only as an exception to that rule. This may be only a minor

change, but all in all it **may lead to Data Protection Authorities gaining less information on data breaches as they used to**. It would be more prudent to keep the current phrasing that states that "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 [or 96] hours after having become aware of it, notify the personal data breach to [the competent authority], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".

Processing of personal data in the terminal equipment of natural persons

Article 88(a) and (b) create various difficulties and cannot ensure legal certainty. Many question are raised:

- **Users' rights**

A significant omission in Article **88a**, compared to Paragraph 5.3, concerns the explanation of the purpose for accessing and storing data on the user's device. First, users are no longer informed about how about the purpose of the use of its data as there **is no longer an obligation to disclose the identity of the "partners" to whom the data will be transmitted. Disclosing such a list is crucial for assessing how intrusive a website is in collecting data and for what purposes.** Additionally, websites often **allow users to choose which partners can receive** their data. However, **this option does not appear to be mandatory under Article 88**a.

- **The consent exception to store or access personal data in the terminal equipment**

Exception for audience measurement Art. 88a(3)(c). Assumption that analytics have low impact on data collection and thus should be consent-exempted does not match t**he reality: the unnecessary amount and granular data collection by very popular analytics services is collected as first-party analytics data in practice and often leaks very sensitive data.** The proposal should consider how recent online tracking developments impact seamless and non-transparent data collection practices: we found that 'Hotjar' audience measurement service collects all the mouse movements, clicks, and keystrokes of the data subject and this is a typical example of an excessive data collection under this exception.

Exception for security. Art. 88a(3)(d) also proposes another exception from consent: "maintaining or restoring the security of a controller's service requested by the data subject or the terminal equipment used for the provision of such service". This raises several questions because it actually contains two exceptions: "security of the service" and "security of the terminal equipment". Security of the service requested by the data subject is a reasonable exception because many services indeed rely on cookies and browser fingerprinting for stronger authentication. S**ecurity of the terminal equipment is questionable**: for example, Noyb and other NGOs are concerned that t**his means allowing companies a broad and massive searching of locally stored data on smartphones, PCs and alik**e. So far, processing for security purposes would often be discussed under Article 6(1)(f) GDPR, which requires the three steps tests (security being generally a legitimate interest, but controllers may not be able to demonstrate that such massive search is indeed "necessary" and especially not "proportionate"). This seems to be extremely invasive for the privacy of the data subjects.

Overall, it is unlikely that these exceptions will provide simplification, as those provision will require guidelines for their application and create, in the meantime, **legal uncertainty**.

- **Scope of article 88(b)**

Article 88b specified that the **online interface is used only for giving consent related to article 88a**. Upon analysing current cookie banners, we can observe while many purposes and consents are provided in accordance with Paragraph 5.3 of the e-Privacy Directive, most are actually related to the GDPR. This is particularly noticeable due to the numerous legitimate opt-out options included in cookie banners. Based on these observations, there is concern that Article 88b may not eliminate cookie banners, as consent and opt-out mechanisms tied to the GDPR remain prevalent in current implementations. This observation could undermine the intended purpose of Article 88b.

- **Art. 88(b) (2) and data subjects' choices**

88 (b) §2, seeks to make mandatory to the controllers to respect the choices made by data subjects in accordance with paragraph 1 i.e. the expression of their personal data choice through the automated and machine-readable indications. However, the provision is not quite clear and one could wonder on the reason why this provision is not the first since all others provision ground on this statement. Moreover, the articulation between the users' choices, consent expression in practice and related rights such as data portability is not laid out creating legal uncertainty.

- **The online interface definition question**

Omnibus proposal's article 3 § 1 refers back the crucial definition of the "online interface" to the one in the DSA (Article 3(m) of Regulation (EU) 2022/2065). Such cross-reference **questions EDPB's and national DPA's jurisdiction over this notion** since Regulation 2022/2065 (Digital Service Act – DSA) empowers competing authorities. Beyond this procedural difficulty, article 3(m) of the DSA defines online interface as "any software, including a website or a part thereof, and applications, including mobile applications". However, Commission's detailed explanation of the Omnibus proposal seems to only target website providers once standards are available. This statement read in combination with Art. 88b§3 – which exempts media service providers- limits article 88b's scope to the sole internet exploration. Such vision allows to see article 88b as an extent of DSA's obligation targeting VLOP and VLOSE, regulated by the DSA, to the GDPR targeting almost all data controllers.

- "**Single click" reject button**

Article 88a(4) and the solution of "single click" reject button, doesn't address all the manipulative design tactics that companies can use to steer users to click accept. Academic research, including our own, shows that multiple "**dark patterns**" are applied today in cookie banners even when "single click" reject button is present:

- highlighting accepts using colors,
- using positioning of the accept in an easy to reach place of the banner, while reject, while present is hard to find;
- using different wording to indicate reject, such as "accept allowed" or "accept necessary" – our research showed that the choice of words plays a very important role in the decision-making of the users
- also, any hints on the fact that the website will stop working if the user rejects is used a lot, and make users believe that they should rather accept. Our research found that many users click on "accept" out of fear that the website will stop working if they click "reject"

None of these issues related to the design, user experience and usability of consent banners is covered in the Omnibus. So this requirement of "single click" is not enough to protect users

from manipulation because **dark patterns** are very powerful. Moreover, in our other work we have found that many EU regulators of ePrivacy have already advanced a lot and propose very concrete design suggestions to protect the users better that could be taken into account by the omnibus proposal.

Article 88-b could be read as an automatic mean to accept the cookies subsequently questioning the result of automatically refusing when a website conditioning its access to the mandatory acceptance of cookies? or to a "consent or pay" mechanism? Will this automation system reinforce the Internet fragmentation with one respecting cookies and the other one respecting privacy ? Will the user after being systematically denied certain access to websites will set up his terminal to accept cookies by default to navigate without any obstacle?

- **Standardisation**

Under article 88-B § 4 the Commission's can delegate to European Standard Organisations the power to define the technical specifications of the "automated and machine-readable means". We do understand that such provision will force the web 2.0 industries to implement an automatic data subjects' choices set-up but it still creates concerns as standardisation organisation tend to disregard privacy and to treat is as a territorial specificity.[2]

Processing in the context of the development and operation of AI

Legitimate interest is a sub-optimal legal basis as far as information self-determination is concerned. As such, it should be used with caution. The proposal on Article 88c however seemingly sidesteps a number of issues while introducing further problems:

- **Absence of details regarding valid legitimate interest of AI developers**.

Article 88c should avoid treating all AI systems uniformly, as the implications of system capabilities for the criteria are considerable. The versatility of generality of general-purpose models makes it difficult to circumscribe a specific legitimate interest. Broadly formulated and speculative interest such as "AI training" or an undefined future "AI technology" cannot constitute a valid legitimate interest. Data controllers must articulate the interest with far greater precision, with a consideration of wider social benefits of the model.[3]

- **Absence of details regarding the requirement of necessity**

In practice, the requirement of necessity requires that the data controller is able to prove that the processing activity will allow the pursuit of the purpose and that there is no less intrusive way of pursuing this purpose[4]. This requirement should be understood in light of the principle of data minimisation, which the article 88c rightfully insists on. However, there are situations where **AI developers cannot determine with any certainty the precise amount of data strictly necessary to fulfill a specific purpose**. Additionally, **data minimisation tools such as anonymisation or personal data filtering may be difficult to adopt due to their impact on model performance**.[5]

---

[2] Julien Rossi & Jonathan Keller, Are internet standard developing organisations data controllers under the GDPR?, *Internet Policy Review*, 2025, 14(3).

[3] Kate Goodloe, A legitimate interest in AI training, *IAPP Opinion*, 2024; Also see Pablo Trigo Kramcsák, Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets ?, *Computer Law & Security Review*, 2023, 48.

[4] EDPB, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, V. 1.0, Adopted on 08/10/2024.

[5] Hannah Ruschemeier, Generative AI and data protection. *Cambridge Forum on AI: Law and Governance*, 2025, 1(6).

- **The proposal lacks technical guidance regarding data subject's rights**

The granular contribution on measures to be deployed by the data controller to tip the scale of the balance of interests in favor of the data controller is most welcomed, but **it omits to mention data deletion requests, for which appropriate avenues should also be provided**. Further, even though legitimate interest was already considered by certain DPAs as the relevant legal basis, **stakeholders have highlighted several issues related to data subject rights implementation in practice**, especially in the context of larger, general-purpose AI models.[6] An example is the question of opt-out avenues in the context of third party data collection as in the case of web scraping.[7]

- **The Balancing of interests is complex**

The larger the scale of AI training and the extent of prior web scraping, the more difficult it becomes for AI developers to tilt the balancing test in their favor.

Extensive processing almost inevitably entails widespread impacts. Considering the extent of AI training, especially, for general-purpose models, security measures need be particularly robust. **Indiscriminate character of data scraping for AI training also impacts the balance of interests in that data subjects may feel that their private life is being monitored.**[8]

Far-reaching risks need be taken into account too. There are documented risks of discrimination and biased outputs due to over-or-under representation in dataset. There is also a risk that some AI tools are weaponised to harass or intimidate individuals, and other long-term risks related to cognitive decline in relation to the use of certain generative AI systems.

- **Read conjointly with the amendment proposed of Article 9 GDPR, the proposal seems to offer a free pass to the incidental processing of sensitive data under the legitimate interest legal basis for training AI systems**

Indiscriminate processing of data produces serious impact on data subjects because sensitive data may also be caught in the training process. This eventuality is addressed elsewhere in the Omnibus and raises additional questions. **Providing for the possibility for residual processing of special categories of data under legitimate interest is a dangerous slippery slope, especially considering the difficulty to satisfy data subjects rights.**

---

[6] NOYB, *Digital Omnibus - First Analysis of Select GDPR and ePrivacy Proposals by the Commission*, 2025, V 3.0, p.76.

[7] Lokke Moerel, EU Digital Omnibus amendments to GDPR to facilitate AI training miss the mark, *IAPP Opinion*, 2026.

[8] EUCJ, 4 july 2023, C-252/21, *Meta vs Bundeskartellamt* § 118.

- **Contradicts the principle of tech neutrality**

By codifying the legality interest as the appropriate legal basis for AI training, the proposal installs a more conciliatory framework of AI technology trained on personal data[9][1]. The term "AI system" is defined very broadly under EU law, which means that the proposed legal basis could end up being applied across a wide range of contexts. Given the aforementioned uncertainties and the reliance on an opt-out mechanism, such breadth risks weakening individuals' data protection rights and overall control over their personal data across the EU.

- **Legal uncertainty remains**

Article 88c contributes very little to legal clarity. Its outcome and the balancing test in particular, depends on the individual circumstances of each case. This indeterminacy is a source of legal uncertainty, which contradicts the rationale behind the digital omnibus.

- **Heavier Workload ahead for Courts and DPAs**

There is no much granularity as regard to the application parameters of legitimate interests to AI contexts. With AI developers in charge of conducting Legitimate interest analysis, **a lot of weight is put on *ex post* forms of control by DPAs and the judiciar**y.

[9] See EUCJ 5 Dec. 2023, C-683/2, *NVSC*.