Warszawa, 22 kwietnia 2026 r.
KL/284/74/ET/2026

Pan
Dariusz Standerski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

w związku z trwającymi pracami nad unijnym pakietem uproszczeń prawa cyfrowego (tzw. Digital Omnibus), Konfederacja Lewiatan, w załączeniu, przesyła stanowisko w rzeczonej sprawie.

Z poważaniem

Marek Górski
Prezydent Konfederacji Lewiatan

Do wiadomości:
1) Pan Mateusz Sztobryn – Zastępca Dyrektora, Departament Projektów i Strategii, Ministerstwo Cyfryzacji
2) Pani Anna Gos – Dyrektorka, Departament Zarządzania Danymi, Ministerstwo Cyfryzacji
3) Pani Katarzyna Prusak-Górniak – Kierownik wydziału, HWPCI, cyberbezpieczeństwo i cyberdyplomacja, Stałe Przedstawicielstwo RP przy Unii Europejskiej

Załącznik: Propozycje poprawek Konfederacji Lewiatan do Digital Omnibus

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla m. st. Warszawy w Warszawie XIII Wydział Gospodarczy

LEWIATAN

Propozycje poprawek Konfederacji Lewiatan do Digital Omnibus

1. Article 4 (1)

Refinement of the definition of personal data (Article 4 (1)) The Omnibus Proposal introduces a constructive approach by linking the definition of "personal data" to the means reasonably available to a controller. To further enhance legal certainty and prevent fragmented interpretations, it would be beneficial for the final text to more fully reflect CJEU case law and Recital 26 of the GDPR. We suggest retaining the Omnibus amendment while specifying that identifiability should be assessed from the entity's perspective, taking into account objective factors such as costs, technological resources, time required for identification, and the specific safeguards applied during processing.

2. Article 22

Calibrating automated decision-making to ensure proportionate application The clarification that automated decisions are permissible under Article 22 when specific conditions are met—even if human intervention is theoretically possible—is a significant step toward modernizing the framework. To ensure this provision remains targeted, we recommend that the final text clarifies the scope of Article 22 GDPR. It should ideally apply to automated decisions that determine a person's legal status or contractual rights, or those that produce a comparably significant and lasting impact on the individual.

In addition, the Omnibus introduces in Recital 38 a requirement that controllers use the "less intrusive" automated processing solution where several equally effective alternatives exist. While the principle is sound, its application to logistics, e-commerce, and digital services requires clarification. In these sectors, a model processing fewer data points may appear less intrusive but may also be less accurate, generating more false positives and greater harm to affected individuals. The Commission, in cooperation with the EDPB, should issue interpretative guidance on how the "less intrusive" standard interacts with decision accuracy and data minimisation in practice.

Furthermore, the revised Article 22(1), point (b), conditions automated decisions authorised by law on the existence of "suitable measures to safeguard the data subject's rights and

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla m. st. Warszawy w Warszawie XIII Wydział Gospodarczy

freedoms and legitimate interests," but provides no indication of how proportionality should be calibrated across different operational contexts. For high-volume, individually low-impact automated decisions characteristic of logistics operations, such as parcel routing, delivery scheduling, or claims triage, proportionate safeguards may take the form of exception-based human review triggered by anomalous outcomes or customer complaints, rather than case-by-case human approval. The final text, or accompanying guidance, should confirm that risk-proportionate safeguard models are permissible, ensuring that the modernised Article 22 delivers legal certainty without imposing operationally unworkable requirements at scale.

3. **Article 88c**

Harmonising the AI Act with Data Protection standards Article 88c plays a pivotal role in aligning the GDPR with the concepts introduced by the AI Act, particularly by recognising legitimate interest as a valid legal basis for AI development. This modernization is essential for creating a clear, EU-wide standard for AI training. In this context, we suggest retaining the Omnibus amendment while streamlining the wording to eliminate potential ambiguities or overlapping requirements, thereby ensuring a more cohesive regulatory environment.

4. **Article 26**

Adjusting the framework for joint controllership (Article 26) While joint controllership was intended for cases of genuine co-determination, expansive interpretations have increasingly turned it into a broad liability framework, leading to legal uncertainty and significant compliance burdens. We propose a targeted amendment to Article 26 to clarify that entities should be regarded as joint controllers only when they actively participate in and exert actual influence over the decisions regarding both the purposes and the means of processing.

5. **GDPR Article 88a vs ePD Article 5(3)**

Consolidating rules to effectively address consent fatigue The current division between the GDPR and the ePrivacy Directive (notably Article 88a GDPR vs. Article 5(3) ePD) continues to foster legal fragmentation and contributes to the growing issue of consent fatigue. Simply shifting certain tracking rules into the GDPR with limited exemptions may not resolve these underlying systemic challenges. A more effective approach would be to fully align Article

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla m. st. Warszawy w Warszawie XIII Wydział Gospodarczy

88a with GDPR legal bases and integrate provisions regarding traffic data and direct marketing entirely within the GDPR framework, rather than maintaining parallel ePrivacy requirements.

Additionally, it's worth noting that the enumerated list of processing purposes exempted from the consent requirement under Article 88a does not address processing operations characteristic of complex online platforms combining different services in a single transaction flow. This omission leaves a significant category of controllers – whose processing activities are closely tied to contract performance rather than to tracking or advertising – in legal uncertainty. The following categories should be addressed via explicit resolution, either in the final text or in binding guidance by the Commission:

(a) Security-related processing: the processing of terminal equipment data for the purpose of risk scoring and authentication necessary to ensure the security of a digital transaction is not included in the Article 88a list. It must be clarified whether such processing falls within the consent exemption for security purposes or requires a separate legal basis under Article 6 GDPR. The current ambiguity is incompatible with the operational requirements of security-critical processing at scale;

(b) Cross-session service continuity: where a user initiates a service interaction on one device and continues or completes it on another, the processing necessary to maintain continuity of that interaction must be explicitly addressed. The proposal does not clarify whether this constitutes processing "strictly necessary for the provision of a service explicitly requested by the user" within the meaning of Article 88a;

(c) User preference storage: the retention of user-selected configuration or preference data on terminal equipment, where stored solely for the purpose of pre-populating those settings in subsequent interactions with the same controller, should be addressed. The current text does not resolve whether preference memory directly ancillary to the performance of a contract requires consent.

Moreover, we appreciate te specific situation and role of the media sector. Even where motivated by the objective of strengthening user control over personal data, the proposed measures must not result in a disproportionate restriction of publishers' ability to finance and effectively operate their digital activities. It is therefore essential to preserve a genuine capacity for publishers to independently obtain and manage user consents at the level of their own services, given that the current legal framework continues to make a wide range of digital functionalities conditional upon user consent. Any limitation of this autonomy

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla m. st. Warszawy w Warszawie XIII Wydział Gospodarczy

LEWIATAN

would weaken the publisher–user relationship and undermine control over content monetisation models. As regards the envisaged “media exemption”, it must not be construed in an unduly narrow manner. In practice, it needs to extend to key technological partners (vendors) that are indispensable for the functioning of digital services, in particular in the areas of advertising, audience measurement and analytics. Absent such coverage, the exemption would remain illusory. The new proposal should not lead to the erosion of “consent or pay” models, which—provided that the requirement of freely given consent is duly met—constitute an important mechanism for financing professional digital journalism.

6. New GDPR article 88a(3)(c)

Article 88a(3)(c) limits the right to store and process personal data for audience measurement purposes only to controllers of the online service, if it is perfomed solely for its own use. This proposal would result in elimination of independent third party audience measurement systems that are fundamental to the online environment (such as JIC – Joint Industry Committees) and limit access to data for indepenedent researchers. This would not only be evidently to the detriment of European internet publishers but also contradictory to art. 24 of EMFA on audience measurement. According to EMFA audience measurement sytems must be transparent, impartial, inclusive, proportional, non-discriminatory, comparable and verifiable. Eliminating joint-controllers from processing personal data for the purpose of audience measurment undermines these priniples and results in creating a “walled garden” for publishers and traditional media. The current proposal favours internal non-audited analytics based on non-transparent rules and methodologies. It would destroy the current statistical and quality audience measurement standard widely accepted in Europe which is essential for publishers.

7. Browser level consent - Article 88b

Article 88b must be deleted. Retaining this provision risks anchoring the Omnibus to a proven-failed architecture, instead of critical updates that the European digital economy needs.

The European Commission is right to target "consent fatigue," but resurrecting browser-level consent in Article 88b ignores the technical failures of past reform efforts and threatens to fracture Europe's digital economy. By recycling an approach that failed in both

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

the 2017 ePrivacy Proposal and the 2023 Cookie Pledge, this mandate introduces profound legal and technical unworkability that directly undermines the ad-supported open internet.

- Article 88b severely degrades the efficiency and value of both personalized and contextual advertising. Research from Implement Consulting Group estimates this centralized approach will drive a 60-65% drop in consent rates, cutting €40-50 billion in value from the ad-supported web. For every additional 1% reduction in the consent rate, annual advertiser revenue is projected to drop by another €600-800 million. The consequences are clear:

    - It forces independent publishers towards paywall models creating a two-tiers internet and undermining the free, open web.
    - It severely degrades the efficiency of a key communication channel, directly undermining core business activity and growth
    - It redirects ad spend away from the open web and directly into the large platforms capable of retaining measurement and personalization capabilities.

- Additionally, Art. 88b fails its primary legal objective: it will not actually reduce cookie banners. A simple "Accept All" setting renewed every six months fails to provide the granular detail required for “informed” consent across millions of unique websites and purposes. Consequently, websites may still be required to display banners to request specific permissions, meaning the number of banners is unlikely to decrease.
- The severe risks have triggered unified pushback across the digital economy. In a joint letter dated February 18, 2026, a broad coalition—including all major EU publishers trade organizations (EPC, NME, ENMA/ENPA), the online advertising sector, advertisers, retailers, and the travel industry—formally rejected Article 88b.
- While the recent EDPB/EDPS Joint Opinion supports this centralized mechanism, their endorsement should be viewed with caution. The Opinion suffers from a massive economic blindspot: because the EDPB operates strictly on a privacy mandate, they entirely ignore the financial damage this mechanism will inflict on Europe's digital economy and media diversity.

  A centralised cookie management system risks undermining the competitiveness of European digital companies, particularly SMEs that rely heavily on advertising tools. By potentially limiting the ability of e-commerce businesses to communicate directly with users to obtain their consent for data processing, it weakens the platform-customer relationship that is fundamental to the digital economy. This relationship enables companies to innovate and compete effectively. Moreover, Article 88b is likely to inadvertently encourage users to apply uniform, blanket privacy settings across all services - regardless of context or trust in individual providers. Such behavior is likely to lead to a structural decline in user consent for data processing and to significantly reduce the flexibility and effectiveness of marketing activities. These effects will disproportionately impact smaller businesses, which depend more heavily on targeted advertising and lack alternative channels to reach customers at scale. In this context, the proposed measures risk conflicting with the EU's broader objectives of strengthening EU competitiveness and fostering innovation within the digital single market.

To address the persistent issue of consent banner proliferation, the regulatory focus must shift from managing the symptoms (cookie banners) to resolving the root cause: over-reliance on consent regardless of the level of risk or harm. The current framework mandates user permission even when the privacy impact is negligible, creating a burden that outweighs the protective benefit.

Instead, the Digital Omnibus should adopt a risk-based approach that expands Art.88a's exemption to contextual advertising and low-risk activities. This would remove the consent obligation for low-impact, non-intrusive activities such as contextual advertising, third-party analytics, ad fraud prevention, and audience measurement. Lifting this requirement would simultaneously promote privacy-preserving practices while diminishing user consent fatigue by naturally reducing consent banners. This approach would ensure consent is still required, but reserved where user choice and control matter most – such as for personalised advertising.

8. **Article 9(2)(k) and Article 9(5)**

The introduction of Article 9(2)(k) is a necessary step, creating a derogation for the processing of Special Categories of Data (SCD) in the context of AI system and model development. However, both Recital 33 and the operative safeguards in the new paragraph 5 make clear that this derogation applies specifically to residual SCD, data that inadvertently exists in training, testing, or validation datasets despite not being necessary for the purpose of processing. The derogation's safeguard framework reflects this: paragraph 5 requires controllers to avoid collecting SCD, remove it when identified, and only where removal requires disproportionate effort, protect it from being used to produce outputs or disclosed to third parties. Recital 33 explicitly confirms that where SCD processing is necessary for the purpose, the controller should rely on the existing derogations under Article 9(2)(a)–(j).

This creates a significant regulatory gap. Bias detection, measurement, and correction in AI systems require the deliberate retention and analysis of SCD, precisely the scenario excluded from Article 9(2)(k). Yet none of the existing derogations under Article 9(2)(a)–(j) provides a clear and reliable legal basis for this processing in a commercial AI context. Point (g), substantial public interest, requires a basis in Member State law, which remains uneven and uncertain across the EU. Point (j), scientific research, is narrowly scoped and does not comfortably extend to operational bias testing by commercial entities. The result is that Recital 31 of the Omnibus recognises processing personal data to detect and remove bias as a legitimate interest under Article 6, but the regulation provides no corresponding Article 9 pathway enabling the SCD processing that effective bias detection requires.

We recommend that the final text address this gap through one of two approaches. The first option would be to amend Article 9(5) to include an explicit carve-out permitting the retention and controlled processing of SCD for the purpose of bias detection, measurement, and correction, subject to strict safeguards: purpose limitation to bias assessment, access controls, data minimisation to what is necessary for that assessment, and deletion once the objective has been fulfilled. The second option would be to introduce a new point under Article 9(2), for example, a point (m) creating a standalone derogation for bias-related SCD processing, distinct from the residual-data regime of point (k). Either approach would close the gap between the Omnibus's stated objective of supporting bias mitigation (Recital 31) and its operative provisions, which currently lack a workable legal basis for the SCD processing that bias mitigation requires.

Furthermore, the interaction between Article 9(2)(k) and the new Article 88c should be clarified. Article 88c establishes that personal data processing for AI development may constitute a legitimate interest under Article 6(1)(f), but addresses only the Article 6 legal basis and is silent on Article 9. The final text should confirm that the legitimate interest recognised in Article 88c is understood to encompass bias detection activities, and that the Article 9 framework provides a corresponding pathway for the SCD processing such activities require.

Article 4(8)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla m. st. Warszawy w Warszawie XIII Wydział Gospodarczy

Article 4(8) of Regulation (EU) 2023/2854, as amended by the Digital Omnibus, introduces a refusal mechanism allowing data holders to decline disclosure of trade secrets where there is a high risk of unlawful acquisition by entities in third-country jurisdictions. The provision requires data holders to demonstrate this risk without, however, specifying the standard of proof, the form, or the frequency of such demonstration. This creates significant legal uncertainty for operators of large-scale connected infrastructure, where the same data categories are continuously generated and subject to recurring access requests. The following clarifications are necessary:

(a) The demonstration requirement must be capable of being discharged on a categorical basis – that is, by reference to the general legal environment of the requesting entity's jurisdiction and the category of requested data – rather than requiring a transaction-by-transaction analysis. Absent this clarification, the mechanism may prove operationally unworkable for high-frequency data environments;

(b) The provision must specify the form, content, and deadline for communicating a refusal and its justification to the requesting party. The current text leaves these elements entirely unaddressed, creating procedural uncertainty;

(c) The provision must clarify the treatment of EU-domiciled entities that are directly or indirectly controlled by third-country entities, given that Recital 13 identifies subsidiary relationships as a relevant factor but the operative text does not translate this into a workable assessment standard.

We recommend that the Commission issue guidance confirming that operational data generated by automated physical infrastructure constitutes data protected as a trade secret within the meaning of Article 2(1) of Directive (EU) 2016/943, where its economic value derives from network-wide aggregation and proprietary processing. Such data includes, but is not limited to, network utilisation patterns, demand distribution models, capacity optimisation parameters, and location performance analytics. The final text should confirm that the demonstration requirement can be discharged by reference to the general legal and enforcement environment of the requesting entity's jurisdiction, rather than requiring transaction-specific analysis.

9. Article 10 – Repeal of Regulation (EU) 2019/1150 (P2B)

The repeal of Regulation (EU) 2019/1150 (the P2B Regulation) is justified by the more comprehensive regulatory framework established by Regulation (EU) 2022/2065 (the Digital Services Act) and Regulation (EU) 2022/1925 (the Digital Markets Act). However, the transition framework established by Article 10(2) – maintaining cross-references to P2B

Regulation provisions until the earlier of amendment in their original acts or 31 December 2032 – creates a prolonged period of regulatory uncertainty for online intermediation service providers.

We recommend taking into advisement the following steps to ensure a smooth transition:

(a) Publication by the Commission of a mapping document identifying for each substantive obligation under the P2B Regulation the corresponding provision of the Digital Services Act or Digital Markets Act that serves as its successor, enabling platform operators to align their compliance frameworks with the applicable law under the post-P2B regime without uncertainty during the transitional period;

(b) Online intermediation service providers that are not 'very large online platforms' within the meaning of the Digital Services Act should receive clear guidance confirming which obligations of the Digital Services Act are applicable to them and in what form, to avoid a situation where P2B repeal inadvertently reduces the transparency and fairness obligations applying to such platforms before the DSA obligations are fully clarified;

(c) The transitional period until 31 December 2032 should be accompanied by a review mechanism allowing earlier alignment, particularly where the cross-referencing legislation can be amended to refer directly to DSA/DMA provisions, in order to reduce the period of regulatory complexity for platform operators managing multiple contractual frameworks.

10. Article 6-9

The single-entry point mechanism as currently drafted seems to not resolve two critical operational ambiguities that should be addressed in the final text or its implementing acts:

(a) Sectoral classification: the text does not specify how entities that simultaneously qualify as important entities under NIS2 and as controllers under GDPR Article 33 are to be classified within the SEP workflow. Without this, the risk of parallel rather than unified reporting procedures is not eliminated;

(b)

(b) Deadline conflict: Article 20 of NIS2 requires preliminary incident notification within 24 hours, while the amended Article 33 GDPR – as proposed in the Digital Omnibus – provides a 96-hour deadline. The SEP cannot in practice function as a unified interface if the underlying deadlines remain misaligned. The final text should resolve this conflict explicitly, either by harmonising the deadlines or by specifying the procedure where a single event triggers both obligations.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla m. st. Warszawy w Warszawie XIII Wydział Gospodarczy