

Warszawa, 9 października 2026 r.  
KL/663/204/ETŚ/2026

Pan  
**Dariusz Standerski**  
Sekretarz Stanu  
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

w związku z trwającymi pracami nad projektem rozporządzenia Digital Omnibus Konfederacja Lewiatan przekazuje w załączeniu stanowisko zawierające uwagi i postulaty dotyczące proponowanych zmian.

Z poważaniem



Marek Górski  
Prezydent Konfederacji Lewiatan

Załącznik: Stanowisko Konfederacji Lewiatan w sprawie projektu rozporządzenia Digital Omnibus

Do wiadomości:

- Pani Katarzyna Prusak-Górniak, Head of Digital Unit, Permanent Representation of the Republic of Poland to the EU in Brussels
- Pan Mateusz Sztobryn, Zastępca Dyrektora, Departament Projektów i Strategii, Ministerstwo Cyfryzacji

member of



member of



Konfederacja Lewiatan  
ul. Zbyszka Cybulskiego 5  
00-727 Warszawa  
tel. +48 22 50 50 860  
repcja@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

## **Remarks of Polish Confederation Lewiatan on Digital Omnibus**

As COREPER considers granting the Irish Presidency a mandate to begin negotiations with the European Parliament on the Digital Omnibus package, we believe the current text still fails to address several key concerns raised by industry. At the same time we want to stress that adopting the Digital Omnibus Package during the Irish Presidency should remain a priority. While this position paper addresses industry concerns and underscores the need to refine specific elements of the text, making these necessary adjustments should not jeopardize closing the Digital Omnibus file within the Irish Presidency's term.

In particular:

### **1. Absence of a cybersecurity handbrake**

The proposal does not include the cybersecurity safeguard requested by industry, which would allow a data holder to refuse a data access request where disclosure would materially increase cybersecurity risks affecting the security, resilience, or integrity of its systems, products, or connected infrastructure. This is a fundamental protection for businesses operating critical digital infrastructure and managing sensitive data environments.

### **2. Pseudonymization and clarity on personal data definition**

If all data is treated as personal data regardless of whether anyone can realistically be identified, then businesses will carry cost and legal risk with no gain in protection while the incentive to invest in privacy-enhancing techniques (PETs) disappears. EU courts have consistently held that whether data is personal depends on who holds it and what that party can realistically do. The new Article 25a codifies that principle, which is one of the most valuable things this file could achieve. However, as drafted, it does not ensure that anonymized data remains outside the scope of the rules. As drafted, sharing pseudonymized data can make it personal data for the sender as well as the recipient. It should be confined to the recipient's own processing - in line with the EDPS v SRB CJEU ruling. Moreover, the test that a person is not identifiable where the likelihood of identification is "insignificant in practice" has been moved out of the article and into a recital. A threshold of that importance belongs in the operative text.

### **3. A workable legal basis for AI**

AI models trained on large and diverse datasets cannot be built on individual consent, a reality that was recognised by the European Data Protection Board (Guidelines on Web Scraping for AI development, para 44). Legitimate interest - which requires a genuine balancing of interests and safeguards - is the basis the GDPR already provides for exactly this

member of



member of



Konfederacja Lewiatan  
ul. Zbyszka Cybulskiego 5  
00-727 Warszawa  
tel. +48 22 50 50 860  
repcja@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

situation. Saying so explicitly gives one EU-wide reference point instead of diverging national and regulator readings. Keeping that provision in the operative text is the right approach. The concern is that Article 88bis as drafted, read together with Recital 33a and its reference to national laws requiring consent, risks making inoperative the very legitimate interest it claims to confirm. Providing that processing “may be carried out for a legitimate interest ... in accordance with Article 6(1)(f)” restates what Article 6(1)(f) already permits, while paragraph 3 adds a standing safeguards obligation that is already inherent in the balancing test. As currently drafted, the reference to the right to object (Art.21) could be read as applying to all GDPR legal bases, in direct opposition to the GDPR core architecture that reserved the application of Art.21 to processing based on legitimate or public interests only. The net effect is additional expectations without additional certainty - the opposite of what a simplification exercise should produce.

#### **4. Ensuring legal certainty for publishers**

It may also be worth considering a clarification tailored to publishers whose professional journalists invest in creating original, high-quality content. Where users are offered a genuine choice between consenting to the relevant processing and accessing such content through an equivalent paid alternative. This would support legal certainty while respecting users’ freedom of choice.

#### **5. Removal of the outdated restrictions under Articles 6 and 9 of the ePrivacy Directive**

The Digital Omnibus should remove Articles 6 and 9 of the ePrivacy Directive and bring the processing of traffic and location data fully within the GDPR framework. These sector-specific provisions impose rigid purpose limitations and consent requirements that prevent electronic communications providers from relying on the GDPR’s risk-based legal grounds and safeguards, including for fraud prevention, cybersecurity, service improvement and the development of data-driven and AI-enabled solutions. Maintaining a parallel regime creates regulatory fragmentation, places telecom operators at a disadvantage compared with functionally equivalent digital services and discourages privacy-enhancing innovation. A single, technology-neutral GDPR framework would preserve strong protection for users while improving legal certainty, consistency and effective enforcement.

#### **6. Insufficient protection of trade secrets**

The changes introduced by the Council do not adequately address longstanding concerns regarding the protection of trade secrets under the Data Act. On the contrary, the newly proposed requirement for the European Commission to issue guidelines on how to assess “serious economic damage” and the enforceability of trade secret protections in third countries risks further narrowing the already limited protections available to data holders.

member of



member of



Konfederacja Lewiatan  
ul. Zbyszka Cybulskiego 5  
00-727 Warszawa  
tel. +48 22 50 50 860  
repcja@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

While the Council has slightly lowered the evidentiary threshold required for a company to refuse data sharing on trade secret grounds, this adjustment is marginal and does not materially improve the ability of businesses to protect commercially sensitive know-how and intellectual assets.

Trade secret protection thus continues to be treated as a narrow and burdensome exception rather than a fundamental right. Requiring manufacturers to meet unrealistic thresholds creates significant administrative obstacles and leaves proprietary engineering know-how exposed.

Beyond trade secrets, the Council's compromise fails to address other key industry concerns under the Data Act. In particular, it does not provide the legal clarity needed to support the development of AI and digital business models, leaving intact restrictions under Articles 4(13) and 4(14) that prevent manufacturers from using industrial data for these purposes. It also fails to account for the specific characteristics of industrial and B2B software solutions by not exempting industrial SaaS/PaaS from disproportionate cloud switching obligations under Chapter VI.

A growing number of Member States share these concerns. In particular, the Austrian Federal Chancellery's paper of 1 October highlights that the current scope of the Digital Omnibus remains insufficient and calls for more ambitious changes delivering substantive legal clarifications and measurable reductions in administrative burdens. Further work on the Data Act is therefore needed, particularly on trade secret protection, cloud switching and restrictions affecting AI development and product improvement.

## **7. Unworkable exemptions from consent**

Reinstating a consent exemption for contextual advertising in Article 5(3) of the ePrivacy Directive is a welcome step toward fostering privacy-preserving advertising models and reducing consent fatigue across the EU. However, the current Council proposal excludes all personal data and past user activity from the exemption and therefore creates practical blockers. Under the GDPR, basic technical signals like ads view counts legally constitute "personal data," while essential functions such as frequency capping or attribution require looking at what happened moments earlier during a user's single navigation. Consequently, the exemption will be useless, and publishers will still have to rely on consent banners just to serve and measure contextual ads. To make the exemption workable, contextual advertising should simply be defined as advertising that is not based on profiling (i.e., that doesn't create user profiles or use previously created profiles) so it can cover display and technical functions, while ensuring that all forms of personalized ad remain strictly scoped out.

member of



BUSINESSatOECD

member of



Konfederacja Lewiatan  
ul. Zbyszka Cybulskiego 5  
00-727 Warszawa  
tel. +48 22 50 50 860  
repcja@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

We also welcome the dual-exemption framework for and third-party audience measurement and for audience measurement under the EMFA. However, requiring the former to be "anonymous" and not only "aggregated" makes the exemption unworkable, as any audience measurement needs to count individual visits and interactions to be relevant. We encourage the Council to keep the "aggregated data" market standard as it provides sufficient protection against user profiling and is consistent with the EMFA exemption, which requires only pseudonymization.

While this position paper addresses industry concerns and underscores the need to refine specific elements of the Digital Omnibus text, making these necessary adjustments should not jeopardize closing the Digital Omnibus file within the Irish Presidency's term

***KL/663/204/ETŚ/2026***

member of



**BUSINESS**atOECD

member of



Konfederacja Lewiatan  
ul. Zbyszka Cybulskiego 5  
00-727 Warszawa  
tel. +48 22 50 50 860  
repcja@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