LEWIATAN

Polish Confederation Lewiatan position paper on the proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 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)
2025/0360 (COD)

I. General remarks

- Lewiatan welcomes the Digital Omnibus proposals, which are a good starting point toward simplifying EU tech rules, cutting red tape, and boosting competitiveness. We believe that some of the provisions, such as adjusting the timeline for the application of high-risk AI rules, as well as adapting GDPR to support the development of AI, go in the right direction.
- We welcome the streamlining and consolidation of the different pieces of legislation into one single Data Act. This is an important first step in creating more consistency across the different scopes and definitions and improving readability for companies, and further reinforces the protection of trade secrets. The creation of a single and unified framework for public sector data re-use is also a positive step to minimize the overlaps and could help foster data sharing in that context.
- However, we believe that overall, the proposals fail to address the competitiveness gaps that industry and heads of state have identified and called for the EU to be much more ambitious:
    - The proposed changes on AI and innovation need to reflect the urgency of addressing Europe's dramatic competitiveness gap. Indeed, many heads of state and European CEOs have strongly called the European Commission to adopt bold reforms on the AI Act and GDPR:
        - Over 60 of Europe's largest companies—representing millions of workers and families—recently issued an urgent statement pleading with the EU to simplify digital regulations, including the AI Act and the GDPR (source: EU Champions initiative launch).
        - 19 member states called for systematic review of all EU regulations to identify rules that are superfluous, excessive, or unbalanced as well as a thorough examination of the entire acquis of EU rules to determine whether

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

regulations are still fit for purpose to meet the European Competitiveness goals

- More ambition is also needed in the area of cybersecurity, where the complexity of existing rules requires simplification measures that go beyond simply streamlining incident reporting obligations.

II. Detailed remarks

1. On the AI Act

Lewiatan welcomes the extended deadlines to implement high-risk requirements to allow more time for harmonised standards to be developed. We would specifically call for the EU to create a separate legislative proposal specifically for these timeline extensions in order to avoid delays in adoption and further confusion for industry.
We also **welcome the limitation of registration obligations** (Deletion of Art 49(2) of the AI Act), clarifying that AI systems which are used in high-risk areas but for which the provider has concluded that they are not high-risk as they are only used for narrow or procedural tasks will be exempted from registration. This would not only reduce administrative burden but also security risks.

We call for **further simplification of the presumption of conformity with cybersecurity obligations under the CRA and the AI Act**: companies should be able to demonstrate conformity under both legal acts through a common conformity assessment, not just through certification.

2. On the privacy framework (GDPR and ePD)

Regarding GDPR and ePrivacy, confirming legitimate interests for the development of AI models and systems as well as providing clarity in the concepts of personal data and anonymisation as recently confirmed by the CJEU is constructive, and we encourage EU co-legislators to support these provisions. We also believe that the proposed changes to Article 22 enabling automated decision-making under safeguards will provide much needed flexibility and clarification to support the development of AI innovations like Agentic AI, particularly in a B2B context, for example for Know-Your-Customer (KYC) verifications. Further clarification must be added to clarify the threshold confirmed by the Court of Justice in C-634/21 (SCHUFA) that legal or similarly significant effects arise only where the decision decisively determines the position of the data subject or has a comparably significant impact.

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

However, the Omnibus misses the chance to strengthen risk-based proportionality across the GDPR and embed a clear mandate to regard innovation and economic impact, in particular for data protection authorities. Such simplification and clarification are essential, in particular in the context of AI development and innovation.

The Omnibus also fails to repair a cookie regime that imposes friction without commensurate benefits and repeats past mistakes by introducing consent management tools which boost complexity. Aligning ePrivacy fully with GDPR legal bases, avoiding duplicating the current problems under the GDPR and also bringing traffic data and direct marketing under the GDPR are essential measures to ease consent fatigue, enable safety-enhancing use cases, and support growth through accurate measurement of ad effectiveness.

Structural upgrades are also needed to secure coherence and predictability. A truly explicit risk-based approach in GDPR would support proportional and practical compliance in fast-evolving technologies. A centralized EU interpretative body by expanding the scope of implementing act and delegated act powers by the Commission, who is legally equipped and accountable under direct CJEU oversight, could bring the uniformity, consistency and economic awareness that businesses need to plan, invest, and scale in Europe.

Legal Certainty & Innovation Enablement:

- The entity-specific personal data definition clarifies that identifiability is contextual, reducing ambiguity and aligning with CJEU jurisprudence. Ensure certainty by anchoring interpretation with the EC together with anonymisation and pseudonymisation assessments (Art.41.a).
- The proposal attempts to codify CJEU case law by stating that data is not personal to an entity that 'does not have the means, the use of which would be reasonably likely' to identify a person. While correct, this approach still leaves room for interpretation, especially for large companies. Large entities have vast data and technology resources at their disposal, which could lead to the interpretation that 'reasonably likely' means much more for us than for SMEs. This creates the risk that, in practice, very little data will be considered non-personal. More objective criteria or so-called 'safe harbours' for pseudonymised data should be introduced. The regulation should clearly indicate that data pseudonymised using strong, widely recognised cryptographic standards (where the key is stored separately and secured) are treated as non-personal by default for entities that do not have access to the key. Such a change would significantly facilitate the use of data for analysis, innovation and training of AI models without falling under the GDPR regime.

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

- AI innovation exemptions are retained: processing residual Special Category Data (SCD) in AI development is allowed (Art. 9(2)(k)), and AI training is explicitly recognized as a Legitimate Interest (Art. 88c). Further technology neutral exemptions must be added recognizing Legitimate Interest; Contractual Necessity and Public Interest, subject to appropriate safeguards.
- Automated decision-making is clarified (Art. 22), confirming that automated decisions are permissible when conditions are met, even if human decision-making is possible. Further clarification must be added to clarify the threshold confirmed by the Court of Justice in C-634/21 (SCHUFA) that legal or similarly significant effects arise only where the decision decisively determines the position of the data subject or has a comparably significant impact.
- We welcome the amendments to Article 9 of the GDPR aimed at the possibility of processing biometric data to verify the identity of the data subject without the need to obtain the consent of the data subject, in a situation where the biometric data is controlled by the data subject.

At the same time, we point to the need to open up this provision more widely, i.e. to allow the processing of biometric data without the need to obtain consent – both for the purpose of identity verification and to prevent crimes (frauds) committed against banks and other financial institutions and their customers

But Technical and Regulatory Complexity and Missed Opportunities for Broader Reform:

- The proposal to limit SCD processing to data that "directly reveals" sensitive information was not adopted, maintaining legal complexity for inference-based data. The amendment to SCD and Data Concerning Health need to be restored.

- Legitimate Interest is not a general legal basis for SCD processing beyond AI, missing a chance for broader, responsible data use. Ensure technology neutrality.

- The dual regime for personal vs. non-personal data (GDPR Art. 88a vs. ePD 5(3)) creates classification uncertainty and implementation complexity. Consent as bottleneck persists: even though cookie/tracking rules are now governed under GDPR (Art. 88a), eliminating the dual regime, consent persists. Art. 5(3) needs to be fully withdrawn and Art. 88a fully

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

aligned with GDPR recognizing all legal bases, to avoid replicating the consent fatigue issue and creating a separate consent regime under the GDPR.

- We are concerned that Omnibus creates a higher protection status for non personal data on a terminal equipment than personal data.
- It should provide more incentives for privacy preserving practices. For example an additional exception to consent where access to non personal information on a terminal equipment is required to deliver a feature that would otherwise have required the server side processing of personal data. This would result in a better a privacy outcome while also achieving the simplification Goal. Simplification should be a reward for good privacy practices not bad.
- It should not undermine the ability to provide best privacy by default settings.

- Regulation of traffic data and direct marketing remains split between GDPR and ePrivacy, perpetuating duplication and compliance burdens. Bring traffic data and direct marketing also under the GDPR regime and withdraw under ePrivacy.

- Use of data for AI training (Art. 3, GDPR amendment) - The proposal recognises data processing for AI training as a 'legitimate interest', which is a step in the right direction. However, it still requires a balancing test, which is complicated and fraught with legal uncertainty for large data sets. A clearer legal basis should be created for the processing of personal data for the purposes of training, testing and validating AI systems, especially with regard to removing bias. Consideration could be given consider introducing a specific exception in Article 6 of the GDPR that would allow such processing subject to strict technical and organisational measures, such as anonymisation, pseudonymisation and data minimisation, without the need to carry out a balancing test each time.

- **New conditions for entities with significant market power (Article 1, amendment to the Data Act):**

The proposal introduces the possibility for the public sector to impose higher fees or special conditions for the re-use of public data on 'very large enterprises'. This definition is vague and could be applied arbitrarily to companies such as ours, which are major market players. The criteria defining a 'very large enterprise' must be objective, transparent and uniform across the EU. They should be linked to specific indicators, such

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

as gatekeeper status within the meaning of the DMA, and not left to the free interpretation of national authorities. Otherwise, there is a risk of market fragmentation and discrimination against large companies.

Risk-Based Proportionality & Reduced Burden:

- The threshold for breach notification is raised to "high risk" (Art. 33), reducing unnecessary reporting.

- Data subject rights abuse prevention is strengthened: Art. 12(5) now covers exploitation of rights for non-protection purposes, with a lower burden of proof for "excessive" requests.

- Risk-based transparency (Art. 13(4)) exempts low-risk, clear relationships from certain transparency obligations.

- AI-specific SCD exemptions introduce graduated safeguards (avoid → remove → protect).

- Biometric verification exception (Art. 9(2)(l)) allows user-controlled authentication.

But Missed Principle-Based Reforms:

- The risk-based approach is not embedded as a core principle in Article 5, so absolutist interpretations may persist in non-harmonized areas.

- There is no explicit innovation mandate for DPAs; innovation and economic impact are not explicit GDPR objectives.

- Risk-based proportionality, balancing fundamental rights and related interests, and taking into consideration innovation and economic impact, must be horizontally strengthened in accordance with Art.52 of the Fundamental Rights Charter to ensure coherence, prevent gaps and the relocation of current issues.

Harmonization & Simplification:

- DPIA harmonization (Art. 35) replaces 40+ national lists with a single EU standard.

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

- A common breach template and a unified list of “high risk” breach circumstances are to be developed by the EDPB.

- Unified cybersecurity reporting is achieved through the ENISA single-entry point.

- Single Entry Point (SEP) – Articles 6–9. The SEP concept is excellent, but its success depends on technical implementation. If the platform is not fully interoperable with companies' internal systems (e.g. via API), its usefulness will be limited. There is also a risk that national supervisory authorities will require additional information beyond the standard form, undermining the idea of ‘report once’. The Regulation should require ENISA to create open, well-documented APIs for SEP, enabling the automation of reports from corporate systems. It should also be made clear that the SEP reporting form is comprehensive and that national authorities cannot request additional information as part of the same initial incident report.

- Terminal equipment consolidation: cookie/tracking rules are now governed under GDPR (Art. 88a), eliminating the dual regime. Cookies rules are now brought under GDPR (and, thus, the One-Stop-Shop). Consent is still required, but four specific low-risk purposes, including audience measurement and security purposes, have been exempted from consent.

- ePrivacy security obligations are consolidated under GDPR and NIS2.

- The temporary effect of certain P2B provisions is extended to 31 Dec 2032.

But Fragmentation & Incomplete Harmonization:

- Despite harmonized DPIA and breach rules, 40+ DPAs retain discretion over other provisions, risking continued divergent interpretations and enforcement.

- Centralization is limited in scope: only DPIAs and breach templates benefit from unified standards, leaving other key GDPR concepts open to national divergence.

- To ensure simplification, sustainably address current issues and respond to the Draghi report call for harmonisation - the implementing act powers for the EC must be expanded to relevant definitions, key concepts and provisions to ensure uniform interpretation. Delegated act powers for the EC should be included to enable future proofing.

- **Draft article 88b GDPR (art. 3(15) of the draft Digital Omnibus)**

According to the proposed Article 88b GDPR, providers of web browsers, which are not SMEs, must provide the technical means for users to give or refuse consent and exercise the right to object via automated and machine-readable means. This obligation facilitates the introduction of centralised cookie management mechanisms, often controlled by browsers or operating systems.

Introduction of a centralised cookie management mechanisms will have an important impact on European market:

- The introduction of centralised consent mechanisms, as required by Article 88b, would severely damage Europe's wider digital economy, including SMEs.
- Users prefer to maintain agency over their data collection choices, often making distinct decisions for each website or app based on the content or service. Therefore, a centralised consent management system may not be suitable for all user preferences, as it diminishes this level of control.
- It would prevent European companies from engaging directly with users to obtain consent or apply other legal bases to process the data necessary to operate, innovate, and finance their products and services.
- This removes the capability of European companies to manage consent, effectively creating a new intermediary (the browser/central system) between a publisher and their audience, risking the creation of new gatekeepers without proper governance reflection.
- Existing gatekeepers (who often control the relevant browsers/operating systems) would continue to obtain consent on a large scale, putting European companies at a structural and competitive disadvantage and undoing progress made by the Digital Markets Act.
- It would sanctify consent as the only basis to access personal data, freezing the status quo, despite the European framework offering multiple legal bases and exceptions.

- Consolidating consent state and identifiers into a central repository would create a high-value target and single point of vulnerability/failure for cyber attacks across all dependent services.
- It introduces fundamental changes without an impact assessment, leading to high costs for European businesses without evidence of simplifying compliance or improving user outcomes.

European institutions should avoid introducing centralised consent management systems. Such systems have previously failed to gain agreement during ePrivacy Regulation negotiations and met widespread disapproval during the "Cookie-Pledge Initiative". It is essential that European website owners and digital businesses maintain the operational and legal capacity to request and manage user consent, or apply other legal bases, directly at the website level, as this direct relationship with users is of paramount importance.

Mandating browsers to introduce automated, machine-readable consent mechanisms (as per proposed Article 88b GDPR) acts as a gateway to damaging centralised cookie management systems. These systems would concentrate power, undermine the competitiveness of European digital and media companies, threaten media plurality, and create new security risks, ultimately running contrary to the core objectives of enhancing Europe's competitiveness and innovation.

The browser-based, machine-readable consent mandate "consent management tools" (Art. 88b) is seen as technically unworkable and likely to perpetuate compliance complexity. We propose to delete Art.88b given its proven legal, technical, political and economical unfeasibility (e.g. Cookie pledge).

- **Draft article 88c GDPR (art. 3(15) of the draft Digital Omnibus)**

Aligning the AI Act and GDPR

A primary concern is the unstable legal basis for AI training, as the common reliance on legitimate interest is highly evaluative and creates legal uncertainty. Additionally, the principle of data minimisation is difficult to adhere to, given that AI development often

requires extensive datasets, making it hard for companies to assess the minimum necessary amount of data. We welcome the targeted amendments to the AI Act and the proposed clarification to the GDPR, particularly the confirmation that AI system development and training may rely on legitimate interest as a legal basis. However, it is essential to ensure that the rules governing the use of legitimate interest for AI development and training remain clear, coherent, and readily understandable for businesses.

Finally, the right to be forgotten (Art. 17 GDPR) is technically challenging to execute for AI models. While input data can be deleted, erasing data from the models themselves is technically complex, akin to deleting specific data from backup systems. A pragmatic solution is to adjust Article 17 GDPR to include an exception based on the disproportion between the actions required (e.g., full model erasure) and the effects/risks. Establishing these adjustments and a separate legal basis would provide much-needed clarity on proper legal grounds for AI data processing.

3. On Data Governance

We welcome the Commission's proposal to merge provisions from the Data Governance Act, Free Flow of Non-Personal Data Regulation, and Open Data Directive into the Data Act, creating a single, streamlined framework. It repeals outdated regulations while maintaining core principles such as the prohibition of data localization. This will help simplify compliance by reducing fragmentation and preserving key principles. International data flows are a cornerstone of the data economy, and companies rely on them to enhance their global competitiveness, develop products, and gain insights on issues that are global in nature. Data localization requirements, intentional or unintentional, will also hurt sectors that do not participate heavily in international trade.

Remove the ability to differentiate conditions for "gatekeepers" in the public sector data reuse context - The provision would ultimately limit choices, including through higher fees, and create unnecessary additional complexity in the data sharing value chain, which would be detrimental to reaching the EU's goals to foster data sharing and data re-use. A likely net effect of such

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

provisions will be to limit the ability of EU businesses to access cutting edge and innovative data analytics, especially in the context of AI development and deployment.

We also **welcome the clarification on trade secrets safeguards**, thereby protecting companies' IP in cross-border contexts, and we encourage EU co-legislators to uphold these provisions.

However, we are **concerned about some provisions that would significantly alter the regime for cloud switching**. Indeed, paragraph 15 of the Commission's proposal includes a provision into the Data Act setting that a cloud provider may include termination charges in contracts of fixed duration other than IaaS (Infrastructure-as-a-Service) contracts. However, the adopted Data Act reaffirmed contractual freedom, stating that parties may agree on reasonable termination charges in line with Union or national law. This reflects common practice in B2B relationships, where enterprise customers understand that committing to a fixed-term contract is generally more cost-efficient but entails termination charges if ended early. These charges are negotiated and clearly stipulated in the contract upfront.
Further flexibility on some of the technical and contractual requirements would be helpful to better reflect feasibility of switching scenarios. We would also call for careful consideration regarding the development of an upcoming repository of harmonized standards and/or common specifications. Digital services are in constant state of evolution while the disruptive innovation that creates whole new classes of digital services forces older technologies to become obsolete. Careful consideration needs to be given to how such open interoperability specifications are identified to ensure a future proof framework.

4. On Cybersecurity

The Single Entry Point (SEP) for reporting is a good first step towards harmonizing incident notifications to the relevant national competent authority.
We view the introduction of a Single-Entry Point (SEP) for incident reporting, to be developed and managed by ENISA, as a promising first step toward streamlining reporting obligations across key EU cybersecurity and digital regulations. By allowing organizations to submit a single notification automatically routed to relevant national authorities, the SEP has the potential to reduce administrative complexity, prevent duplicative or inconsistent queries, and ensure that critical information promptly reaches the appropriate authorities. In order for the SEP to realize its full potential to further materially enhance the simplification and alignment of incident

reporting across multiple digital domains, we recommend taking the following aspects into consideration:

- **Use the CRA Single Reporting Platform (SRP) as the foundation for the Omnibus Single Entry Point (SEP)** – To ensure a truly unified and coherent EU-level reporting architecture, the SEP's scope should be expanded to include incidents notified under the Cyber Resilience Act (CRA). While Article 4(1) allows ENISA to rely on the CRA SRP, without explicit alignment, there is a risk that the CRA SRP and SEP evolve as parallel systems. We recommend that co-legislators designate the CRA Single Reporting Platform as the model and shared infrastructure for the Single-Entry Point (SEP), creating a coherent and unified EU-level incident reporting framework.

- **Integrate AI Act serious incident reporting into the SEP mechanism** – Allowing providers to submit a single interoperable notification that is automatically routed to the relevant authorities and national market-surveillance authorities (MSAs) would prevent up to 27 parallel investigations and inconsistent or uninformed queries. It can also offer clear efficiency and oversight benefits for governments and national authorities. By routing notifications through a single-entry point with national CSIRTs docked in, authorities can more easily identify cross-sectoral trends, detect cross-border risks, and coordinate responses. This approach also eliminates the need for Member States to manually disambiguate overlapping legislative requirements and accelerates information-sharing between various cyber, AI, and product-safety regulators. Over time, it could support a more coherent understanding of emerging risks, including clarifying the boundary between model-level and system-level incidents.

- **Develop a secure and efficient mechanism within SEP to facilitate follow-up communications** – We further recommend incorporating within this platform a secure and efficient mechanism for follow-up communications. A centralized system for responding to regulatory inquiries would allow competent authorities to share information, reduce redundant requests, and ensure consistency in messaging. This enhancement would improve regulatory coordination and ease the compliance burden on stakeholders.

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

- **Harmonize definitions, timelines, and thresholds for incident reporting** – For the SEP to effectively fulfil its goal of reducing administrative burden and legal uncertainty, it must be accompanied by harmonization of definitions, reporting timelines, and thresholds across EU frameworks and aligned with international best practices. This combination would create a coherent, streamlined, and operationally efficient incident reporting system. In line with this, we recommend ENISA to be tasked with conducting a comprehensive study mapping overlaps, redundancies, and inconsistencies across EU regulatory reporting requirements, to inform the design of harmonized templates, aligned procedures, and interoperable technical standards for the SEP. Key areas for alignment include:

    - **Definitions of cybersecurity incidents**: Uniform definitions are essential to clarify when cyber reporting obligations are triggered, what constitutes a reportable incident, and to prevent duplicative notifications across frameworks.

    - **Reporting timelines**: Aligning deadlines for different stages of reporting, such as early-warning alerts versus full notifications, and harmonizing reporting channels across jurisdictions would simplify compliance and strengthen early-warning capabilities.

    - **Reporting thresholds**: Standardized criteria for what constitutes a reportable incident would streamline incident response, reduce operational costs, and allow organizations to focus on effective mitigation.

- ***Ensure ENISA is adequately resourced to deliver on its expanded technical and operational responsibilities*** – The Omnibus tasks ENISA with managing the technical and operational aspects of the SEP, ensuring its security, reliability, and interoperability across Member States. Without commensurate increases in financial and human resources, ENISA's ability to fulfill these responsibilities will remain constrained. We recommend that any additional responsibilities related to the development of SEP are matched with appropriate increased budgetary and staffing allocations, a consideration that should also inform the upcoming Cybersecurity Act revision.

- ***Ensure the development and maintenance of the SEP are driven by structured multi-stakeholder input*** – Recital 44 mandates ENISA to consult the Commission, the CSIRTs

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

Network, and competent authorities on the SEP's technical specifications. To ensure regulatory coherence and practical utility, structured engagement with the private sector should also be embedded into development and ongoing maintenance of the SEP. ENISA should establish a regular consultation mechanism - such as a stakeholder forum or expert group - with opportunities for input through public consultations, written submissions, and technical workshops. Direct engagement with businesses which process and report incident data is essential to design secure, interoperable, and user-friendly reporting mechanisms, strengthen shared cybersecurity responsibility, and mitigate inadvertent compliance burdens.

However, **more simplification is needed in cybersecurity**:

- **The definition of 'main establishment' needs to be harmonized** across cyber legislations: companies should be able to have one main establishment for all cyber legislation.

- **Both NIS2 and CRA are missing liability clauses**: we need to build trust so companies are comfortable sharing information.

- **Overlap of audit and conformity assessment requirements must be addressed in Omnibus, and not in a future Cybersecurity Act (CSA), which will take too much time to be negotiated and implemented**:
    - Companies that are in scope of NIS2, DORA, GDPR, and CRA have to face multiple processes, conformity assessments and audits requirements to demonstrate compliance with each of these regulations. While each regulation has its specificity and scope, a lot of security requirements under one regulation could qualify as compliance with another, particularly among those that are applicable to critical infrastructure (i.e. NIS2 and related sector-specific laws such as DORA). In practice, the lack of a coordinated EU-wide oversight framework has created a fragmented compliance environment, which results in repeated audits where providers must demonstrate the same risk controls to multiple clients throughout the year.
    - Additionally, the harmonization goal of NIS2 is challenged by additional national rules and varying conformity assessment processes required nationally, which would risk further fragmentation. For example, NIS2 requires similar risk management measures across the EU, yet companies would have to undergo multiple conformity assessments in various forms (e.g. certification or third-party audits) in each of the

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

countries they operate, even though this is the same requirement for all member states.

All these processes are resource-intensive and costly, yet do not lead to meaningful improvements in risk management. These inefficiencies ultimately increase costs for end-users.

5. On data transfers to the US and the UK

- The proposal focuses on simplifications within the EU, but does not systematically address the biggest challenge currently facing companies operating globally – legal uncertainty regarding data transfers to third countries, especially to the US (following the Schrems II ruling) and the UK (following Brexit). Although this goes beyond the scope of 'technical' amendments, the Commission should prioritise work on a durable and stable legal framework for data transfers to key trading partners. In the context of this regulation, the role of the European Data Protection Board (EDPB) in issuing binding guidelines on transfer impact assessments (TIAs) could be strengthened to harmonise the approach across the EU.

KL/629/212/ET/2025

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