Position paper on the Digital Omnibus GDPR & Incident Reporting

FEDIL
The Voice of Luxembourg's Industry

Luxembourg, 30 March 2026

Toward a smarter, leaner and more competitive EU Digital framework

Position paper on the Digital Omnibus GDPR & Incident Reporting

I. Introduction and general remarks

Europe's digital regulatory framework is at a turning point. While the GDPR has established a global benchmark for data protection, eight years of implementation have revealed structural issues that now hinder innovation, legal certainty and operational efficiency.

Organizations face overlapping obligations, divergent interpretations across Member States, and administrative burdens that absorb resources without meaningfully improving data protection outcomes.

At the same time, technological developments: AI, cloud infrastructures, pervasive digital services, have outpaced the original architecture of the GDPR.

The Digital Omnibus is therefore an essential and timely exercise. It provides the first meaningful opportunity since 2018 to address known bottlenecks in the GDPR, close interpretative gaps, streamline disproportionate obligations, and align the regulation with today's digital and technological realities.

Updating the GDPR through targeted amendments is not a weakening of data protection, it is a modernization necessary to preserve its credibility, effectiveness and relevance.

Amending the GDPR is beneficial and necessary because:

- Legal uncertainty persists, notably around the definition of personal data, the scope of high-risk processing, DPIA requirements, and the boundaries of ADM, creating fragmented enforcement and interpretative inconsistencies across the EU.
- Administrative burden has grown disproportionately, with companies struggling to comply with obligations that are often unclear, duplicative or misaligned with actual risk.
- The regulation has not kept pace with technological evolution, particularly AI development cycles, fraud-prevention requirements, and real-time digital service operations.
- Cross-regulatory alignment is urgently needed with NIS2, DORA, CER, AI Act and ePrivacy, as the digital acquis has grown into a patchwork of diverging definitions, inconsistent reporting timelines and parallel regimes.
- Businesses require clarity and predictability to innovate, invest and scale digital solutions confidently across the Single Market.

This paper constitutes FEDIL's additional contribution to the Digital Omnibus package focusing specifically on the GDPR-related chapters, including the Single-Entry Point for incident reporting. This contribution complements BusinessEurope's position on the GDPR[1], which FEDIL supports while providing more granular operational feedback and industry perspectives.

[1] https://www.businesseurope.eu/publications/making-gdpr-more-effective-a-businesseurope-position-paper/

II. Key recommendations for a digital framework that works in practice

A. GDPR amendments

1. Narrowing the definition of personal data: clarify to simplify, not complicate

The proposed clarification of what constitutes personal data is a welcome and necessary step forward. It responds to long-standing challenges faced by industry, especially in situations where controllers cannot reasonably identify an individual and are nevertheless subject to fulfill GDPR obligations. A clearer and more risk-based definition can significantly reduce unnecessary administrative burden and better support innovation in the era of AI.

In this context, the shift toward a contextual, risk-based test ("means reasonably likely to be used") is a positive evolution, as it modernizes the GDPR and aligns it with CJEU case law. It offers a more practical approach for determining when data should genuinely be treated as personal.

To fully deliver the intended simplification, the reform must address the following:

- A subjective standard must not undermine legal certainty.
  The concept of "reasonably likely" must be applied in a way that ensures predictability and avoids legal ambiguity. Controllers should not face excessive documentation or continuous reassessment obligations to justify what is, in practice, low-risk processing. Without clear and harmonized guidance at EU level, there is a risk of inconsistent interpretation across Member States, which could undermine the benefits of the reform.
- Alignment with EDPB guidance is essential.
  The EDPB's 2025 Pseudonymization Guidelines[2] already define criteria for assessing identifiability. These must serve as the authoritative reference to avoid conflicting interpretations and ensure uniform application.
- Clear criteria are needed to prevent "legal vacuums" around the concept of reasonable identification.
  Data cannot oscillate between "personal" and "non-personal" depending on contextual changes such as access to additional information. Without legal stability, companies risk retrospective non-compliance. Clarifying criteria for assessing identifiability in line with EDPB and ECJ positions would reduce uncertainty and risk of legal vacuum.
- The reform should reduce administrative burden.
  Clarifying when pseudonymized data falls outside the GDPR should reduce documentation and compliance obligations, helping companies reallocate resources, not force them to document interpretative assessments of identifiability.

FEDIL supports clarification, but only if it strengthens legal certainty, reduces administrative load and compliance costs and prevents fragmentation across the single market.

[2] https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf

2. Processing sensitive data in the context of AI: enables innovation, not obstacles

FEDIL supports the creation of a dedicated legal basis for processing sensitive data in the context of AI, a crucial enabler for fairness, bias detection, and compliance with the AI Act, yet stresses that several conditions attached to the new exemption remain operationally unrealistic and not aligned with the technical and organizational realities of AI development.

The exemption must be workable and proportionate:

- Intentional collection of sensitive data must be allowed under safeguards. Bias detection and fairness assessments often require the intentional and supervised collection of sensitive attributes, carried out under strict safeguards. Prohibiting such intentional collection would directly contradict core requirements of the AI Act and undermine the development of trustworthy and fair AI systems. However, when sensitive data is not intentionally collected but is instead provided to a service provider without the provider knowing the nature of the data, no consent should be required for the provider to process it. In these scenarios, the provider cannot reasonably be expected to identify the data as sensitive in advance, nor redesign systems around information it does not actively seek to collect. Requiring consent in such cases would create legal uncertainty and impose disproportionate obligations with no added benefit for individuals.
- Deletion and anonymization rules must reflect AI development cycles. AI models require long-term dataset retention for auditability, reproducibility and safety validation. Immediate deletion is incompatible with both technical reality and regulatory obligations.
- The exemption must align fully with the AI Act's risk-based framework. GDPR and AI Act cannot impose contradictory obligations. Harmonization must be explicit to avoid legal uncertainty.
- Proportionality should guide the treatment of sensitive data. Some categories may not carry the same risk in controlled environments. A rigid application undermines innovation and produces unnecessary administrative burdens.

A legal basis that cannot be operationalized will not simplify the regulatory environment. It must be practical, proportionate and consistent with the broader digital framework.

FEDIL urges lawmakers to ensure the new legal basis truly enables responsible AI development while maintaining appropriate safeguards, not introducing impracticable constraints.

3. Data Subject Access Request (DSARs) reform: avoid new bureaucracy while tackling abuse

The Omnibus intends to minimize abusive DSARs that impose heavy administrative burdens, particularly in HR and financial sectors. FEDIL supports this objective. However, the proposal introduces vague criteria that risk creating new complexity rather than reducing it. Without clear guidance, companies may end up with more administrative tasks, not fewer.

For this reform to deliver actual simplification:

- Clear, objective definitions of "manifestly excessive" and "not related to data protection" are essential.
  Without harmonized criteria, interpretation will vary across Member States and expose controllers to litigation risk. Companies need certainty to confidently refuse or charge for abusive requests without fear of legal challenge.
- The reform must not trigger broader, more cumbersome DSARs.
  Individuals may enlarge the scope of their requests to avoid rejection, increasing administrative workload.
- No conflict with rights to evidence or algorithmic transparency.
  Any reform must preserve individuals' ability to obtain evidence for legal proceedings and to access information needed to understand automated decisions. DSARs linked to credit scoring or algorithmic explanations must remain fully protected, ensuring transparency obligations are not weakened.
- Proportionality and EU-wide guidelines are indispensable.
  Controllers must have legal certainty when refusing requests, supported by examples reflecting real-world scenarios.

A DSAR reform that introduces new ambiguities would defeat its purpose. Clarification, harmonization and proportionality are needed to ensure it lightens, rather than expands, the compliance burden.

FEDIL supports the reform but insists that DSAR simplification must not compromise transparency where it genuinely matters.

4. New exemptions to the obligation to provide information: a valuable reform that needs precision

Reducing transparency obligations for low-risk processing is a positive step toward administrative simplification. However, the current proposal lacks the clarity needed to ensure consistent application.

To avoid ambiguity and fragmentation:

- Definitions of "data-intensive", "clear and limited scope", and "reasonable grounds" must be precise and measurable.
  Vague concepts risk inconsistent interpretations and undermine EU-wide harmonization. Without operational criteria, organizations will maintain full transparency obligations out of caution.
- Low-risk processing should be broadly exempted.
  Only inherently high-risk scenarios, international transfers, automated decision-making, profiling, should remain subject to full transparency requirements.
- Exemptions must be compatible with sectoral rules such as the DSA.
  Regulatory coherence is essential to avoid duplicate obligations or conflicting interpretations.

- Examples and EU-level guidance are vital.
  Controllers must understand when the exemption applies and how it should be communicated to individuals. Companies need operational clarity, not theoretical concepts.

Exemptions should simplify transparency, not shift uncertainty onto controllers through ill-defined concepts.

FEDIL supports the introduction of targeted exemptions but insists that they must bring meaningful administrative relief while ensuring legal consistency.

5. Automated decision-making: enabling responsible automation while safeguarding competitiveness

Automated decision-making (ADM) has become indispensable to maintaining trust, security and resilience in the digital economy. In an environment where AI-generated fraud, synthetic identities and deepfake-based manipulation evolve at unprecedented speed, companies must be able to deploy fast, reliable and adaptive decision systems. Europe cannot remain competitive if ADM is constrained by outdated interpretations that do not reflect today's operational realities.

The Digital Omnibus provides a welcome clarification by confirming that ADM may be used for contractual purposes even when manual decision-making would have been possible. FEDIL strongly supports this evolution, but stresses that greater flexibility is essential for use cases that directly protect consumers, secure transactions and uphold the integrity of digital markets.

ADM is not about replacing human judgment; it is about enabling companies to act proportionately, rapidly and effectively where real-time response is indispensable. However, artificial delay or forced manual review contradict the operational realities companies face. Fraudsters operate at machine speed. They now rely on AI-generated deepfakes, synthetic identities and falsified documents at scale. These attacks evolve within minutes; requiring human review as the default response is both unrealistic and harmful to European competitiveness. European companies must be empowered to defend themselves at the same pace.

To be effective, FEDIL calls for a more flexible and innovation-friendly ADM framework.

- Introduce a dedicated flexibility clause for fraud, security and abuse prevention.
  ADM must be explicitly authorized for fraud detection, account integrity checks, synthetic identity mitigation and security verification. These scenarios demand instantaneous action. Forcing manual review creates operational blind spots and exposes businesses to escalating AI-driven attacks. A clear legal basis will allow companies to deploy robust safeguards while maintaining high levels of protection for users.

- Prioritize a risk-based and technologically neutral approach.
  Low-risk and security-critical ADM should not be subject to the same constraints as high-impact, fully automated decisions. A proportionate, risk-tiered model aligns with the EU's broader digital strategy and reduces unnecessary administrative burdens while preserving strong rights for individuals.

- Preserve meaningful rights of recourse without operational rigidity.
  Individuals must retain the right to be informed, to seek human review and to contest decisions, but these safeguards should not compromise the real-time functioning of essential protection mechanisms. The Omnibus should ensure that recourse rights complement, rather than impede, the effectiveness of ADM used to protect both consumers and businesses.

- Ensure full coherence between the Omnibus, the GDPR and the AI Act.
  ADM requirements must not contradict risk-management obligations under the AI Act. Regulatory alignment is essential to avoid a dual-compliance burden that would undermine simplification efforts and increase fragmentation across the EU single market.

Greater flexibility in ADM is not a deregulation exercise, it is a structural necessity for safeguarding Europe's digital economy, aligning with Europe's own objectives i.e. protecting consumers, ensuring market integrity and enabling innovation.

In fraud prevention and security contexts, companies face adversaries who exploit regulatory inertia and technical constraints. Europe must equip its businesses with scalable, resilient and future-proof tools, supported by a legal framework that recognizes the speed and sophistication of modern threats.

A pragmatic, risk-based and innovation-friendly ADM regime will strengthen consumer protection, enhance trust, and reinforce Europe's ability to compete globally.

6. Data breach notification: targeted improvements that must align with operational realities

The Digital Omnibus introduces two meaningful adjustments to the GDPR's breach-notification regime: a higher threshold focused on "high-risk" incidents and an extended notification deadline of 96 hours. These changes respond to long-standing industry demands for more proportionality and operational feasibility. However, these improvements will only deliver real simplification if they are implemented coherently with the broader incident-reporting reform, particularly the SEP architecture already addressed in detail in Section A of this position paper.

The extension to 96 hours is strongly welcomed: companies need sufficient time to stabilize systems, assess the scope of an incident, verify facts, and avoid premature or inaccurate reporting.

Centralizing personal data breach notification into the SEP is also a welcomed step towards simplification for organizations.

FEDIL calls for a workable and risk-aligned breach notification regime.

- Clarify the "high-risk" threshold to prevent from unintentionally increasing reporting pressure and avoid fragmented enforcement.
  To ensure that the new "high-risk only" threshold genuinely reduces unnecessary reporting, the concept must be clearly defined, consistently interpreted, and operationalized across all Member States. Without a harmonized and practical definition, national authorities may diverge, undermining legal certainty and organizations risk reverting to defensive over-reporting ("better safe than sorry") or,

conversely, under-reporting due to uncertainty, both scenarios undermining the objective of simplification.

Clear EU-level guidance, supported by concrete examples and uniform criteria, is therefore essential to ensure that companies can apply the threshold confidently and consistently during incident response.

7. Harmonized Data Protection Impact Assessments (DPIAs): a much-needed structural rationalization

The decision to create EU-wide DPIA lists and templates is one of the most promising elements of the Digital Omnibus. For years, divergent national approaches have generated confusion, legal uncertainty and unnecessary administrative burden for companies operating across borders.

FEDIL fully supports this harmonization, but stresses that it must be deep, simple and operational, not merely cosmetic.

To truly reduce the burden, the reform must address four structural requirements:

- A drastic reduction in the number of situations requiring a DPIA.
  A harmonized list that remains overly broad would defeat the purpose of the reform. DPIAs must be restricted to genuinely high-risk scenarios, not routine or low-impact processing. Companies should not be forced into unnecessary assessments that drain resources and provide limited added value.

- Short, usable templates with a strict page cap.
  DPIA templates must be concise, practical and operationally usable. A strict maximum number of pages is indispensable to prevent templates from becoming bureaucratic checklists. Companies need practical tools. The goal is to support structured, risk-based decision-making, not to create administrative exercises detached from reality.

- Full cross-regime coherence across GDPR, AI Act, NIS2, CRA and DORA.
  A DPIA must not be required twice under different regulatory labels for the same processing operation. The Omnibus must ensure mutual recognition of assessments conducted under aligned frameworks. Companies should be able to rely on a single, integrated risk assessment, ensuring consistency and avoiding duplicated effort.

- A dynamic, market-based feedback loop to keep DPIA lists accurate and proportionate.
  Harmonized DPIA lists must not become static or outdated. Risk patterns evolve rapidly, and the regulatory framework must reflect real-world developments. FEDIL therefore calls for a formal feedback loop, whereby supervisory authorities, industry actors, sectoral regulators, and EU bodies (EDPB, ENISA, AI Office) regularly review DPIA lists in light of market experience, incident patterns, technological developments, and empirical evidence.
  This mechanism is essential to prevent lists from drifting toward over-inclusiveness, to adjust criteria when risk levels evolve, and to maintain proportionality over time. Without a structured feedback loop, DPIA obligations risk drifting back into unnecessary expansion, recreating the burden the Omnibus seeks to eliminate.

8. ePrivacy & Cookies reform: simplification cannot create new administrative layers

Integrating the ePrivacy cookie rules into the GDPR could have been a landmark opportunity to finally reduce consent fatigue, simplify compliance, and restore a more innovation-friendly and competitive digital environment.

Instead, FEDL stresses that the current proposal risks producing the opposite effect i.e. a reform that adds complexity, concentrates power in a handful of intermediaries, and imposes heavy new technical obligations without addressing the structural causes of user consent fatigue or administrative burden.

8.1 Article 88a: Exemptions must be broadened to genuinely reduce consent fatigue

Under Article 88a, the list of consent-free scenarios remains extremely narrow, covering only transmission, essential functionality, basic internal analytics and security.

This approach misses the core issue: consent fatigue arises because too many low-risk operations or high-value processing operations still require consent. User fatigue is not caused by the absence of centralized consent mechanisms, but by the over-reliance on consent where risk is minimal.

As long as the exemption list remains limited, banners will continue to proliferate and may even increase, since more processing operations will fall under mandatory consent, regardless of any technical improvements in consent management.

To address this, FEDIL calls for:

- A significantly broader, risk-based exemption list.
  The Omnibus must exempt low-risk, high-utility operations that are essential for service quality, user protection and competitiveness, including:
  - fraud prevention and abuse detection,
  - product diagnostics, maintenance and software updates,
  - security hardening,
  - contextual advertising (non-tracking),
  - aggregated analytics,
  - frequency capping,
  - first-party personalization.

  Expanding exemptions, not adding new interfaces, is the only structural way to reduce consent prompts.

- A proportionate, innovation-friendly system.
  The reform must allow companies, including SMEs, to perform basic analytics and deliver service quality without triggering full consent workflows.

8.2 Article 88b: Centralized, machine-readable consent must be removed

Article 88b introduces a mandatory, machine-readable consent framework, requiring browsers and operating systems (excluding SMEs) to collect, store and transmit users' consent/refusal signals on behalf of all websites. While the Commission's intention to address "cookie banner fatigue" is legitimate, the mechanism raises structural issues far beyond online advertising and would apply across the entire digital ecosystem. This is not simplification: it is the creation of a new consent infrastructure, with profound competition, governance, legal certainty and accountability implications.

This proposal imposes substantial new obligations on companies while creating a new bottleneck in the European digital ecosystem.

FEDIL exposes several structural risks, building on concerns expressed by BusinessEurope :

- It creates privacy gatekeepers with regulatory leverage over consent flows, contradicting the pro-competition spirit of the DMA.
- It undermines purpose-specific consent, a core GDPR requirement, by replacing contextual choice with blanket signals.
- It disadvantages SMEs, depriving them of the ability to engage directly with users and explain the value of their services.
- It creates complex chains of accountability, as controllers remain liable for proving consent validity despite having no control over how signals were obtained.
- It risks technical fragmentation, since browsers may implement signals inconsistently.
- It introduces a two-tier system due to the media carve-out, creating confusion for users and distortions for businesses.

Overall, the mechanism assumes technical standardization can solve deeper structural ambiguities in the interaction between GDPR consent rules and ePrivacy. Without clarifying scope, enforcement, and cross-context interactions, Article 88b risks adding a new compliance layer rather than delivering genuine simplification.

FEDIL strongly warns that mandatory centralized consent management will not reduce user fatigue and will not simplify compliance.

Therefore, to address the identified risks, FEDIL urges the co-legislators to:

- Remove mandatory centralized consent management.
  The browser/OS-level mechanism should not be compulsory. It should be voluntary and based on open, interoperable standards, not a new regulatory regime. On this point, FEDIL fully aligns with BusinessEurope's position calling for the removal of Article 88b from the Digital Omnibus.

- Replace centralization with a risk-based simplification model.
  Instead of outsourcing consent to a small set of intermediaries, the EU should reduce the need for consent by meaningfully expanding Article 88a exemptions for low-risk processing.

- Preserve controller–user transparency and accountability.
  Companies must retain the ability to communicate their value proposition directly to users and document consent in a way that is purpose-specific and legally sound.

- Avoid gatekeeper consolidation.
  The reform must not shift greater structural power to a handful of platform operators who already act as chokepoints in the digital ecosystem.

- Support a comprehensive review via the Digital Fitness Check
  FEDIL supports BusinessEurope proposition. The broader reform of ePrivacy and its interaction with GDPR should be addressed through an evidence-based, holistic review, not through a rushed horizontal obligation introduced in the Digital Omnibus.

A credible simplification reform must practically reduce consent fatigue, maintain legal certainty and support a competitive digital ecosystem aligned with the goals of the Digital Omnibus.

9. Legitimate interest for AI development: a decisive step that must remain workable and risk-based

This provision operates in parallel to the AI-specific exemption for sensitive data outlined in Section 2. While Section 2 addresses the conditions for processing special categories of data, Article 88c provides the general lawful basis for training and improving AI models using non-sensitive personal data. Both must function coherently but address distinct legal challenges.

FEDIL strongly welcomes the introduction of Article 88c GDPR, which explicitly recognizes legitimate interest as a lawful basis for the development, training and operation of AI systems. This reform addresses a longstanding legal bottleneck that has hindered European AI innovation and investment. It also aligns with key EU priorities, from competitiveness to data access, and reflects the core objective of the Digital Omnibus: clarity, proportionality and simplification.

However, the effectiveness of Article 88c will depend on its technical feasibility, its coherence with the AI Act, and its ability to support legitimate, low-risk innovation without creating new operational burdens.

To achieve this, FEDIL calls for:

- Restore neutrality between consent and legitimate interest.
  Legitimate interest must be equally valid and operational as consent, even where consent could theoretically be obtained. This avoids turning consent into a default bureaucratic fallback and preserves proportionality.

- Interpret "necessity" in a way that reflects real AI development cycles.
  The Omnibus must explicitly state that "necessity" includes iterative training loops, long-term data retention for auditability and safety checks, continuous fine-tuning and model improvement. Without this, companies face counterproductive delete-and-recollect cycles that undermine quality, security and competitiveness.

- Calibrate transparency and opt-out rights to prevent security and fraud-detection blind spots.
  New obligations must be technically feasible and explicitly conditioned by: "*where technically feasible and reasonable.*" Enhanced transparency must not require disclosing training methods, thresholds or model characteristics that could facilitate exploitation. The right to object must be structured to prevent malicious actors from systematically excluding themselves from datasets, thereby weakening fraud-prevention capabilities.

- Explicitly list "safe and legitimate" purposes where legitimate interest is presumed proportionate.
  To ensure legal certainty, FEDIL recommends listing in Article 88c that legitimate interest presumptively applies to fraud prevention and abuse detection, security and account integrity, bias mitigation, safety validation, model optimization and accuracy improvement, and low risk training operations essential for service quality. This reduces uncertainty and prevents unnecessary reliance on consent.

- Prevent national fragmentation and gold-plating.
  Member States must not be allowed to reintroduce consent requirements or impose additional safeguards. A harmonized, EU-wide approach is essential for legal certainty, cross-border AI development and central to the Single Market.

Article 88c could turn into a strategic enabler for Europe's AI ecosystem. But, only a calibrated, evidence-based approach will allow Europe to develop trustworthy, secure and globally competitive AI, while preserving fundamental rights and ensuring a coherent Digital Single Market.

B. Incident management

1. Incident reporting & Single-entry point (SEP): simplification must be structural, not superficial

The Single-Entry Point (SEP) has the potential to reduce fragmentation and could be transformative for companies. FEDIL supports this objective in principle, as it aims to simplify and reduce regulatory complexity arising from the coexistence of multiple, inconsistent incident-reporting regimes. However, **simplification should not be reduced to technical centralization alone**. Centralizing submissions without harmonizing the underlying rules does not simplify compliance, it simply shifts complexity into a single platform while leaving companies with the same interpretative challenges. This means companies still face multiple deadlines, thresholds and definitions across NIS2, GDPR, DORA, CER and eIDAS, now forced through a single portal that does not solve their inconsistency.

To become a genuine simplification tool, the SEP must rest on a foundation of harmonized concepts and operational clarity.

Position paper on the Digital Omnibus GDPR & Incident Reporting

For the SEP to deliver real simplification, it must go further. FEDIL therefore calls for :

- Legal certainty that reporting through a single channel fulfils all obligations. The essential condition is legal certainty: once an incident is reported through one recognized channel, the reporting obligation must be considered fully fulfilled, and organizations must not be required, or exposed, to parallel or duplicate notifications under other pieces of legislation.
  The “report once, share many and fulfil all” principle is indispensable to avoid duplication, reduce administrative burden and ensure that the SEP delivers genuine operational simplification. However, a degree of flexibility in reporting channels should be considered, allowing entities, where appropriate, to report either via the SEP (for instance in cross-border or multi-regime incidents) or via a national reporting channel.

- Template customization by regulatory regime, designed for crisis situations.
  A “one template fits all” approach will not work. Templates must prioritize "box-ticking" logic and essential information enabling rapid reporting, not legal complexity. Automatic routing should remain transparent, allowing organizations to retain visibility on which authorities receive the notification. Companies need rapid, intuitive forms that mirror real incident workflows.

- Fully aligned and unified reporting timelines.
  New reporting deadlines must be identical across frameworks. A single, consistent timeline would prevent errors, reduce stress on crisis teams and significantly decrease compliance workload.
  Additionally, in the spirit of simplification objective of the Digital Omnibus, a unique timeline for reporting obligations across regulations which provide for incident reporting to the SEP should be considered. However, timelines should reasonably allow to carry out the necessary inspections and investigations, taking into account the urgency of the matter and operational realities organizations are facing when mitigating an incident.

- Guaranteed technical continuity, resilience and fallback channels.
  A centralized system introduces systemic risk if unavailable during major incidents. It must not become a single point of failure (SPOF). Mandatory redundancy, fallback mechanisms, offline alternatives and legal protection in cases of SEP downtime are essential for business continuity.

- Integration of CRA and AI Act reporting.
  Excluding these regimes would reintroduce fragmentation. A true “report once, share many” system must cover all relevant digital regulations that rely on incident notification.

- Mandate ENISA to streamline and align reporting obligations.
  ENISA should be tasked with systematically identifying gaps, overlaps, inconsistencies and redundant reporting obligations across EU digital regulations, and proposing concrete convergence measures. This mandate would ensure the SEP evolves into a genuinely harmonized, simplified and coherent reporting framework, rather than an additional administrative layer.

Position paper on the Digital Omnibus GDPR & Incident Reporting

A SEP that does not reduce the number of decisions companies must take during an incident is not a simplification, it is an additional administrative layer. Only a SEP that rationalizes and harmonizes obligations will meaningfully reduce administrative burden and strengthen Europe's cyber-resilience.

FEDIL urges co-legislators to ensure the SEP becomes an instrument of real regulatory rationalization.

-.-.-.-.-.-

FEDIL, the Voice of Luxembourg's Industry
7, rue Alcide de Gasperi
P.O. Box 1304, L-1013 Luxembourg
E.: fedil@fedil.lu – T.: (+352) 435366 -1