EU Digital Package:

ABBL position on the Single-Entry Point (SEP) for Incident and Breach Reporting and on the Proposal for a Regulation Amending the AI Act

Author(s): Andrey Martovoy, Amandine Laurent, Galina Miroshnichenko
Date: 10 March 2026
EU Transparency register: 3505006282-58

Summary

ABBL welcomes the Digital Fitness Check as an opportunity to address the cumulative impact of overlapping EU digital rules on regulated sectors. From the perspective of financial institutions, the main sources of complexity are not digital interfaces as such, but fragmented legal definitions, diverging notification triggers, parallel assessment obligations, and overlapping supervisory processes across GDPR, NIS2, DORA, the AI Act and, increasingly, the Cyber Resilience Act.

ABBL supports the Single-Entry Point (SEP) for incident and breach reporting, provided it delivers genuine structural simplification. The SEP should become the sole reporting channel under GDPR, NIS2 and DORA, replacing parallel reporting channels rather than adding a new layer. At the same time, supervisory competences of the relevant authorities must be fully preserved. The EU should progressively harmonise key definitions and triggers across the digital rulebook, including “incident”, “major ICT incident”, “personal data breach”, “significant incident” and “high risk”, so that one factual event leads to one legal assessment and one reporting obligation. ABBL also supports extending the GDPR breach notification deadline to 96 hours, clarifying the notion of “awareness”, and developing a modular common breach notification template.

For the financial sector, DORA must remain the *lex specialis*. The Fitness Check should therefore examine where horizontal digital legislation overlaps with sector-specific financial regulation without creating additional supervisory complexities. ABBL supports reconsidering certain DORA incident classification criteria, notably “geographical spread” and “service downtime”, where they drive reporting without necessarily reflecting cyber severity. ABBL also calls for broader proportionality under DORA, beyond micro-enterprises, to better reflect the operational profile of small and low-risk entities, and for clarification of Article 16 DORA for SNI investment firms.

ABBL strongly supports simplification through re-use across regimes. Financial institutions are increasingly required to conduct overlapping assessments under GDPR, the AI Act, DORA and

other frameworks. The EU should therefore move towards a single, modular digital risk and impact assessment framework that can be re-used across legal regimes.

On AI, ABBL supports the objectives of the Digital Omnibus on AI, but stresses that legal certainty remains essential. The unchanged definition of an AI system remains a major source of uncertainty for the financial sector. The AI Act should explicitly exclude traditional deterministic statistical techniques, such as linear and logistic regression and similar rule-based statistical models, from the definition of AI systems. ABBL also supports a clearer and more predictable implementation timeline for high-risk AI obligations, including a delay for Annex III obligations until August 2028. Financial use cases should be differentiated more clearly: fraud prevention and AML tools should not be automatically treated as high-risk, while models already validated under prudential frameworks should not face duplicative obligations. The EU should also clarify the criteria for when a deployer becomes a provider and ensure sector-led supervision for financial services, with strong coordination between the AI Office, financial supervisors and data protection authorities.

More broadly, ABBL encourages continued consolidation of the digital acquis, removal of redundant instruments and greater use of directly applicable regulations. The Digital Fitness Check should focus on coherence, proportionality and competitiveness, while preserving high standards of resilience, data protection and fundamental rights.

ABBL Position on the Single-Entry Point (SEP) for Incident and Breach Reporting

1. Executive Summary

The ABBL welcomes the European Commission's ambition to simplify and rationalise the EU digital regulatory framework in support of competitiveness, resilience and innovation. The proposed introduction of a Single-Entry Point (SEP) for incident and breach reporting under the Digital Omnibus represents a potentially important step towards reducing fragmentation across the General Data Protection Regulation (GDPR), the NIS2 Directive and the Digital Operational Resilience Act (DORA).

However, ABBL stresses that technical streamlining alone will not deliver genuine simplification. Based on the operational experience of financial institutions, the main drivers of complexity lie in fragmented legal definitions, diverging notification triggers and parallel assessment obligations across multiple regulatory frameworks rather than the absence of a common reporting interface.

Effective simplification requires a structural approach to regulatory coherence. In practice, financial institutions currently face overlapping obligations under several EU legal acts, including the GDPR, NIS2 Directive, DORA and the Cyber Resilience Act. This fragmentation

often requires multiple legal assessments and parallel supervisory interactions for the same incident.

ABBL therefore considers that the Single-Entry Point can only achieve its stated objectives if it is implemented as part of a broader effort to simplify the EU digital rulebook through unified legal concepts, proportional implementation and clear recognition of sectoral frameworks such as DORA as *lex specialis* for the financial sector.

2. ABBL's General Position on the Single-Entry Point

ABBL supports the principle of a Single-Entry Point provided that it constitutes a structural simplification of the regulatory framework rather than an additional procedural layer. It is unclear whether the Single-Entry Point would replace incident reporting to individual competent authorities as this is not legally stated within the Omnibus legislation. ABBL would not support the addition of a Single-Entry Point alongside existing reporting under DORA as this would constitute duplication without any benefit to the financial sector.

ABBL welcomes the Commission's objective of introducing a "report once, share many" model for incident reporting. Financial institutions currently face multiple reporting obligations triggered by the same operational event, requiring notifications under several EU legal acts and often to several competent authorities. The introduction of a Single-Entry Point therefore represents an important opportunity to significantly reduce administrative burden and improve the efficiency of incident management processes.

Experience from financial institutions demonstrates that meaningful simplification occurs when a single incident leads to one legal qualification, one reporting obligation and one coherent supervisory dialogue. By contrast, merely aligning reporting formats or timelines while maintaining multiple legal regimes risks re-labelling complexity rather than eliminating it.

3. Conditions for ABBL Support of the SEP

3.1 The SEP must be the sole reporting channel

At present, a single cyber or data-related incident may trigger multiple reporting obligations under EU and national frameworks, requiring separate legal analyses, different templates, diverging timelines and engagement with multiple authorities.

ABBL considers that the SEP can only fulfil its purpose if it is explicitly recognised in EU law as the sole reporting mechanism under GDPR, NIS2 and DORA. Existing parallel notification channels should be formally replaced rather than maintained alongside the SEP. Transitional arrangements should be clearly defined, strictly time-limited and designed to avoid dual reporting obligations.

Without exclusivity, the SEP risks becoming an additional compliance checkpoint and undermining confidence in the simplification agenda.

3.2 Legal certainty through unified definitions, triggers and assessments

Financial institutions consistently report that the most resource-intensive aspect of incident handling is not the preparation of reports, but the need to perform multiple parallel legal assessments for the same event.

ABBL therefore calls for unified definitions of core concepts such as “incident”, “major ICT incident”, “personal data breach” and “high risk” across the relevant EU legal acts. Notification triggers should be aligned so that a single factual assessment leads to a single reporting obligation. The regulatory framework should recognise one legal qualification per incident, with downstream re-use across supervisory regimes.

We note that certain DORA criteria, such as “geographical spread” and “service downtime,” drive higher levels of reporting despite those two criteria not being related to the severity of a cyber incident. ABBL encourages further simplification of incident reporting and supports ensuring that reports relate to incidents that may require regulatory intervention. A removal or reconsideration of those two criteria would improve DORA reporting for in-scope financial institutions.

ABBL therefore calls for the progressive harmonisation of key definitions and reporting triggers across the EU cybersecurity and digital regulatory framework. Core concepts such as “incident”, “major ICT incident”, “personal data breach”, “significant incident” and “high risk” should rely on compatible legal criteria in order to ensure that a single factual event leads to a single legal assessment and one reporting obligation.

Without such harmonisation, institutions remain required to perform parallel legal assessments under different legal acts, significantly increasing compliance costs while providing limited additional supervisory value.

4. GDPR-Specific Considerations

4.1 Extension of the notification deadline to 96 hours and clarification of the notion of “awareness”

For complex incidents involving third-party providers, cross-border operations or evolving forensic findings, the current 72-hour deadline often forces premature reporting based on incomplete information. This can lead to inconsistent risk assessments and repeated follow-up communications.

ABBL supports the proposed extension to 96 hours as more operationally realistic and conducive to higher-quality notifications. This extension should be accompanied by clear guidance on the notion of “awareness” to ensure consistent application across Member States.

4.2 Qualification of "high risk" personal data breaches

The qualification of "high risk" is inherently contextual and depends on multiple factors, including data categories, volumes, mitigation measures and the specific risk profile of the institution. Rigid thresholds or prescriptive lists risk encouraging over-reporting and defensive compliance practices.

ABBL strongly supports a risk-based and contextual approach. Guidance should rely on illustrative non-binding examples rather than binding thresholds, allowing sufficient flexibility to reflect the evolving understanding of an incident as investigations progress.

4.3 Common breach notification template

ABBL supports the development of a common notification template, provided that it is modular, case-specific (i.e. risk-based and conditional on the type and the nature of the incident), and allows for progressive submission of information as it becomes available.

5. NIS2 and DORA Considerations

5.1 Governance and role of ENISA

ABBL recognises ENISA's suitability as a technical operator of the SEP infrastructure.

5.2 Proper coordination among all relevant authorities

ABBL therefore considers it essential that governance arrangements clearly define responsibilities, data access rights and follow-up processes, and ensure strong involvement of financial authorities such as the EBA, ESMA and national supervisors. The SEP should make sure that every European authority and national competent authorities receive all necessary information in due time to proceed with their respective supervisory obligations. The SEP has to be used for all types and directions of communications: from the in-scope entities to authorities and from authorities to in-scope entities. The ultimate goal is to avoid the duplication of reporting to various authorities especially in cases when the incident is transversal and cross-border.

6. Digital Fitness Check and Further Simplification

ABBL strongly supports the underlying philosophy of the Digital Omnibus, namely simplification through unification. Experience from financial institutions confirms that aligning multiple regimes does not eliminate duplication, whereas unifying or repealing overlapping rules does.

The SEP should therefore be seen as a catalyst for deeper integration rather than an endpoint in itself.

6.1 Incident and breach reporting

ABBL encourages the Commission to move towards a single EU incident and breach reporting regime with a common taxonomy, unified legal classification and the designation of a lead supervisory authority per incident.

6.2 Limits of the current simplified regime under DORA

In practice, very few financial entities qualify as micro-enterprises, meaning that many small and low-risk institutions are subject to the same obligations as larger banks. This creates disproportionate compliance costs without corresponding resilience benefits.

ABBL supports extending proportionality beyond micro-enterprises in the financial services sector to include small enterprises, based on risk-based criteria rather than purely quantitative thresholds.

6.3 Investment firms and Article 16 DORA

Investment firms classified as Small and Non-Interconnected (SNI) under the IFR/IFD framework often face uncertainty regarding the application of Article 16 DORA.

ABBL calls for explicit EU-level clarification on the application of Article 16 to SNI investment firms, alignment between DORA and existing prudential classifications, and consideration of lighter eligibility criteria reflecting actual operational risk.

6.4 Risk and impact assessments

Organisations are currently required to perform parallel assessments under GDPR, the AI Act, DORA and the Digital Services Act, despite significant overlap in technical requirements. ABBL supports the development of a single, modular digital risk and impact assessment framework allowing reuse across regulatory regimes.

6.5 Cyber Resilience Act

DORA was specifically designed to harmonise ICT risk management within the financial sector, reflecting sector-specific risks and governance structures. Overlaying DORA with parallel or competing regimes risks undermining its coherence. The Digital Omnibus allows simplification and the recognition of cyber incident reporting under DORA. ABBL recommends the following amendment to ensure CRA reporting does not duplicate with DORA reports for the same incident.

Article 8 from EU Digital Omnibus – Amendments to Regulation (EU) 2022/2554:

- Article 19 of Regulation (EU) 2022/2554 (DORA) is amended as follows:
- 3. In paragraph 1, the following sub-paragraph is added:

'When a financial entity notifies a major ICT-related incident pursuant to this Article 19(1), the reporting of the financial entity under Article 19(1) of Regulation (EU) 2022/2554 shall constitute reporting of information under Article 14(3) of Regulation (EU) 2024/2847.'

ABBL supports exempting the financial sector from the Cyber Resilience Act where DORA already applies, in order to avoid double regulation of banking applications, payment ATMs and other products with digital elements.

ABBL reiterates that DORA must remain the *lex specialis* for the financial sector. Financial institutions that are subject to DORA should be exempted from CRA.

6.6 Continued consolidation of the digital acquis

ABBL encourages the Commission to continue consolidating the digital acquis by repealing obsolete or redundant instruments, prioritising directly applicable regulations and maintaining the Digital Fitness Check as a permanent simplification tool.

7. Conclusion

ABBL considers the Single-Entry Point an important step towards simplifying the EU digital regulatory framework, but one that must be embedded within a broader effort to address structural overlaps across the EU digital acquis. To deliver on its objectives, it must replace parallel reporting regimes, rely on unified legal concepts, respect sectoral specificities and embed proportionality at its core.

Excessive regulatory layering risks diverting resources away from operational resilience and innovation towards administrative compliance. A coherent and streamlined EU digital rulebook is therefore essential not only for regulatory clarity but also for the global competitiveness of Europe's financial sector.

Only through structural unification rather than incremental alignment will the EU achieve a digital regulatory framework that is simpler, more coherent and globally competitive.

ABBL Position Paper on the Proposal for a Regulation Amending the AI Act

Executive Summary

The Luxembourg Bankers' Association (ABBL) welcomes the European Commission's Regulation proposal (the "Digital Omnibus on AI"), amending Regulation (EU) 2024/1689 (the "AI Act"), as regards the simplification of the implementation of harmonised rules on artificial intelligence. ABBL supports the overarching objective of reducing unnecessary administrative burden, while preserving a high level of protection for consumer fundamental rights, financial stability, and innovation.

As a highly regulated sector that has long relied on advanced data analytics and AI-driven tools, the Luxembourg banking sector operates within robust prudential, governance, and data protection frameworks. In this context, simplification should primarily aim at avoiding regulatory duplication, ensuring legal certainty, and enabling proportional, risk-based implementation. While the Digital Omnibus on AI introduces a number of improvements, ABBL considers that several aspects require further clarification or adjustment to ensure predictability, supervisory coherence, and a level playing field across Member States.

1. General Assessment of the Digital Omnibus on AI

ABBL acknowledges the Commission's effort to address practical implementation challenges identified since the entry into force of the AI Act, notably delays in the availability of harmonised standards, guidance, and national supervisory mechanisms. The proposal rightly recognises that these delays, if unaddressed, could undermine effective compliance.

At the same time, ABBL notes that the simplification effect of the Omnibus is nuanced in practice. While some obligations are streamlined, new areas of uncertainty are introduced, in particular through conditional application timelines, reliance on future guidance, and unresolved questions around roles, supervision, and the interaction with sectoral legislation.

In particular, the unchanged definition of an AI system remains one of the most significant sources of legal uncertainty for the financial sector, risking divergent national interpretations, uneven compliance costs, and fragmentation of the Single Market. While Commission guidelines provide some clarification, their non-binding nature does not ensure consistent application, particularly for long-established techniques such as linear or logistic regressions.

ABBL therefore calls on legislators to introduce a binding clarification within the AI Act explicitly excluding traditional deterministic statistical techniques from the definition of an AI system. In particular, well-established analytical methods such as linear regression, logistic regression and other deterministic statistical models used within predefined rule-based decision frameworks should not be considered AI systems for the purposes of the Regulation.

Such clarification would significantly improve legal certainty and avoid unnecessary regulatory overlap with existing prudential frameworks governing model development, validation and governance in the financial sector.

2. High-Risk AI Systems and Implementation Timelines

2.1 Conditional application mechanism

ABBL welcomes the acknowledgment that high-risk AI obligations cannot be effectively applied without supporting standards, common specifications, and guidance. Linking the application of high-risk obligations to the availability of such tools is conceptually sound.

However, ABBL is concerned that the proposed mechanism introduces significant uncertainty. The triggering of obligations depends on the timely publication of the final text and availability of compliance tools confirmed by the Commission, without clear criteria or a defined timeline. In the absence of such a decision, institutions must still plan for the original application dates under the AI Act.

Against this background, ABBL considers that legal certainty would be significantly improved through a clear implementation date and by extending the delay period for the application of obligation applicable to high-risk AI systems under Annex III to August 2028.

Without such clarity, financial institutions face difficulties in budget planning, IT development cycles, compliance certainty and prioritisation of AI use cases.

2.2 Financial Sector Use Cases

ABBL stresses the importance of differentiating between financial use cases that pose high risks to fundamental rights and those that might be considered as high-risk and that are already subject to stringent prudential and conduct supervision. In particular:

- fraud prevention and AML-related AI tools should not be automatically classified as high-risk, given their protective function and existing oversight;
- credit scoring and creditworthiness assessment systems may remain in scope, subject to proportionate requirements and clear supervisory expectations;
- models already validated under prudential frameworks (e.g. Internal Ratings-Based models) should not be subject to duplicative AI Act obligations.

In addition, the sector would benefit from dedicated guidance on the deployment of agentic AI systems and the establishment of appropriate governance frameworks, given their growing use and the specific challenges they raise for human oversight, explainability and accountability.

3. AI Literacy

ABBL welcomes the proposed shift of the general AI literacy obligation from individual providers and deployers to the Commission and Member States, while maintaining targeted training obligations for staff involved in the oversight of high-risk AI systems.

This approach better reflects operational realities and avoids a one-size-fits-all obligation. However, ABBL cautions against the risk of fragmentation, as AI literacy initiatives may diverge significantly across Member States. Enhanced coordination at EU level would therefore be necessary to ensure consistent expectations and avoid regulatory arbitrage.

Luxembourg banks remain committed to internal training for governance, risk management, and compliance purposes, independently of regulatory obligations.

4. Data Protection, Bias Detection and Fairness

4.1 Use of Special Categories of Data

ABBL welcomes the explicit legal basis introduced for the processing of special categories of personal data for bias detection and correction, which reflects operational realities and the need to identify discriminatory effects.

Nevertheless, ABBL notes inconsistencies between the recitals and the operative provisions, notably as regards the extension of this legal basis beyond high-risk AI systems. Clearer and more consistent drafting is needed to provide legal certainty.

4.2 Alignment with Other Digital Legislation

ABBL asks for stronger coherence between the AI Act and other digital and financial legislation, including GDPR, DORA, and sectoral supervisory frameworks. In particular, alignment between AI Act fundamental rights impact assessments and GDPR data protection impact assessments would significantly reduce duplication.

5. Roles, Responsibilities and Supervisory Architecture

5.1 Provider vs Deployer

ABBL notes that the Digital Omnibus on AI does not clarify when modifications to an AI system result in a deployer becoming a provider. This uncertainty is particularly relevant for common banking practices such as:

- retrieval-augmented generation using additional national regulatory or supervisory layers;
- fine-tuning models to meet jurisdiction-specific legal requirements;
- white-labelling deployment;
- extensive system prompting or configuration.

Clear thresholds for "substantial modification" are essential to avoid over-regulation, whereby institutions risk triggering provider obligations merely by adapting systems to meet other legal requirements.

5.2 Transparency in Self-Assessment of Non-High-Risk Systems

ABBL supports the exemption from AI database registration for Annex III systems assessed as non-high-risk, as this reduces administrative burden. However, where a provider relies on such self-assessment, deployers should receive a concise summary of the classification and its reasoning.

This limited transparency safeguard would enhance legal certainty and allow deployers to properly assess their own compliance obligations, without undermining the simplification objective.

5.3 Supervisory Coordination

ABBL is concerned about the potential fragmentation of supervision, especially where a single AI system may fall simultaneously under the remit of financial national and European supervisors, data protection authorities, and the AI Office.

For financial institutions, ABBL strongly supports a sector-led supervisory approach, whereby existing financial supervisors act as lead authorities for AI systems used in the financial sector. These authorities already possess deep knowledge of institutions' governance, risk management, and outsourcing arrangements, and are best placed to ensure coherent oversight.

Formal coordination mechanisms between the AI Office, financial supervisors, and data protection authorities would be essential to avoid overlapping investigations, conflicting guidance, and duplicative sanctions.

This is particularly relevant in Luxembourg, where financial institutions operate cross-border and are already subject to intensive, coordinated supervision.

6. Penalties and Proportionality

ABBL shares concerns that the level of penalties under the AI Act, combined with legal uncertainty, may discourage innovation and lead to overly conservative deployment decisions.

ABBL is in favor of:

- a more proportionate calibration of penalties;
- prevention of cumulative sanctions across overlapping regulatory regimes;
- clear enforcement coordination to ensure predictability and fairness.

7. Conclusions and Recommendations

ABBL supports the objectives of the Digital Omnibus on AI and welcomes several of its proposed simplification measures. To ensure that these objectives are fully achieved in practice, ABBL calls on co-legislators to:

- enhance legal certainty around implementation timelines and conditional triggers;
- provide clear definition of AI systems, a clearer differentiation of high-risk financial use cases and an explicit exclusion of long-established techniques such as linear or logistic regression;
- ensure consistency and coherence with existing financial and data protection frameworks;
- clarify roles and supervisory responsibilities, with a sector-led approach for financial services;
- clarify the criteria under which a deployer becomes a provider of AI systems;
- require providers to share with deployers a summary of the self-assessment for non-high risk AI systems;
- maintain proportionality in enforcement and penalties.

With these adjustments, the Digital Omnibus on AI can become a meaningful step towards an innovation-friendly, coherent, and legally certain AI framework that supports both competitiveness and trust in the European financial sector.