

EBF position on the European Commission's proposal for a Digital Omnibus Regulation: Single-Entry Point (SEP)

Executive Summary

The EBF supports the European Commission's efforts to simplify the EU digital regulatory framework and welcomes initiatives that can help streamline cybersecurity incident reporting. The current situation is characterised by significant complexity resulting from incident reporting requirements established in a variety of legal acts, addressed to a variety of authorities and set in different timelines, templates and taxonomies. This fragmentation and overlap between horizontal and sectorial acts, carries high (and to an extent redundant) compliance burdens, leading to an over-commitment of resources that could otherwise be used in more productive ways, supporting the competitiveness of European financial institutions globally by directing cybersecurity expertise toward risks management and incidents handling instead of reporting.

The Digital Omnibus Regulation is a welcome first step to simplification, but it should mark the beginning of a broader digital fitness check rather than being an endpoint. We note that the interaction between horizontal requirements and sector-specific rules in digital often carries legal uncertainty and operational challenges, given that the financial sector is (rightfully) a heavily regulated one. Any simplification efforts should therefore deliver a tangible and measurable reduction in administrative burden.

Also, in a context where rapid response is essential to address cyber threats effectively, further complexity must be avoided. The proposed EU Single-Entry Point for incident notifications risks adding one more layer to an already established process nationally. In this sense, it would be very useful if the Commission pursued alternative simplification solutions that enhance clarity and streamline the existing frameworks, for example, by aligning the templates and terminology/taxonomy across legal acts and sectors and removing overlapping regimes that require the same incident to be reported more than once.

1. Single Entry Point: Centralising incident notifications

The proposed Single-Entry Point would not, in itself, resolve the core sources of reporting complexity. Even where notifications are channeled through a single platform, entities would still need to assess and comply with different legal thresholds, timelines, and reporting conditions under the relevant Union frameworks. As long as these underlying obligations remain divergent, organisations will continue to operate complex internal classification and escalation processes, which substantially limits the simplification effect intended by the SEP.

For the financial sector, ICT-security and incident-reporting requirements are already governed by the EU level framework, notably DORA and secondary legal acts stemming from it. The concern is therefore that a horizontal single-entry point could duplicate implementation processes already in place, which are aligned according to each Member

State's reporting portals. Any simplification initiative should build on existing requirements and preserve the role of competent financial authorities within the sectoral framework.

It is to be noted that there is an uneven level of maturity of national incident reporting ecosystems across Member States. In several jurisdictions, existing national and sector-specific reporting mechanisms are already well-established, operationally efficient, and trusted by entities. In such cases, any EU-level action should aim to create synergies with existing structures and ensure that it doesn't disrupt or duplicate them. At the same time, in countries where incident reporting frameworks are less mature, efforts should focus on supporting operational improvements and promoting convergence in those requirements, obligations, and processes.

As mentioned already, meaningful simplification requires more than a new reporting tool. It requires an appropriate legal basis to align, where necessary, the underlying reporting obligations across the frameworks within the scope of the SEP. Without such legal adjustments, centralising an interface risks creating an additional reporting point without removing the legal and operational complexity that entities currently face in some member states.

1.1. Responsibilities and liability issues related to risks

While new Article 23a (2) of the NIS2 Directive (Article 6 of the Digital Omnibus) lays out ENISA's responsibilities for ensuring technical, operational and organisational measures, these are limited to managing the risks posed to the security of the single-entry point. It is therefore unclear from the text who would be responsible for receiving, processing, and forwarding reports in a timely manner, and thus responsible for ensuring the confidentiality, integrity, and availability of the information processed via the SEP. This creates a risk that reports submitted via the SEP may be delayed or queries will remain unresolved.

It is therefore necessary to introduce a clause about liability in relation to operational management of such single-entry point, including its technical functioning.

Am n°	Article	Text proposed by the Commission	Amendment proposed
	23a NIS2 Directive	(2) ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. ENISA shall take into account the sensitivity	(2) ENISA shall implement appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of the single-entry point and to ensure the confidentiality, integrity, and availability of the information submitted, processed, or disseminated therein. The measures shall follow a risk-based approach and cover the entire lifecycle of the single entry point, including its development, establishment, maintenance, and continuous secure operation. These

			measures shall, at a minimum, address: (a) the security of the physical and logical infrastructure; (b) incident handling and business continuity management; (c) access control and identity management for authorised users.
--	--	--	---

Am n°	Recital	Text proposed by the Commission	Amendment proposed
	New		(xx) In line with the principle of administrative simplification and the 'report-once' policy, it is necessary to avoid duplicative reporting obligations for financial entities that are already subject to stringent operational resilience requirements. Where a financial entity submits an incident report under Regulation (EU) 2022/2554 [DORA], that submission should be considered sufficient to satisfy the reporting requirements under the Regulation (EU) 2024/2847 [CRA]. This approach ensures regulatory coherence, legal clarity and reduces the compliance burden on the financial sector.

1.2. Consultation with competent authorities and a call for public consultation

We welcome the proposal, under Article 6 of Digital Omnibus, mandating ENISA to adopt specifications on the technical, operational and organisational measures related to the Single-Entry Point. We suggest an additional clarification in relation to the public consultation requirement. In financial sector, we positively note the good practices of the European Supervisory Authorities (ESAs), which hold transparent public consultations prior to adopting technical measures in the form of Regulatory Technical Standards (RTSs). Such requirement for a transparent consultation should be added to the new Article 23a(3) of NIS2.

Am n°	Article	Text proposed by the Commission	Amendment proposed
	23a NIS2 Directive	(3) ENISA shall provide and implement the specifications on the technical, operational and organisation measures	(3) ENISA shall provide and implement the specifications on the technical, operational and organisation measures regarding the

		regarding the establishment, maintenance and secure operation of the single-entry point. ENISA shall develop the specifications in cooperation with the Commission, the CSIRT Network and the competent authorities under the Union legal acts referred to in paragraph (1).	establishment, maintenance and secure operation of the single-entry point. ENISA shall develop these specifications, following a prior public consultation with the relevant stakeholders , in cooperation with the Commission, the CSIRT Network and the competent authorities under the Union legal acts referred to in paragraph (1), develop the specifications .
--	--	--	--

Am n°	Recital	Text proposed by the Commission	Amendment proposed
	New		(xx) The establishment and operation of a single-entry point represent a critical technical milestone for the Union's cybersecurity related incidents notification framework. To ensure that the specifications developed by ENISA are technically robust, future-proof, and operationally viable, it is essential that the drafting process remains open and transparent. Therefore, ENISA should consult not only with national authorities but also with relevant industries representatives.

2. Additional suggestions for simplification

The Digital Omnibus should build a coherent digital regulatory system that integrates horizontal acts with sector-specific having the status of *lex specialis*.

We note that the duplication of outcomes and scope between DORA and the CRA are extensive. All financial services offered through digital channels - such as mobile banking apps, insurance apps, payment cards, ATMs, and point-of-sale terminals – are already regulated under DORA, which imposes stringent and comprehensive requirements on financial entities' ICT systems and services, including ICT-related reporting requirements.

As stated by in recital 24 of DORA:

" [...] this Regulation [DORA] should lay down a robust ICT-related incident reporting regime whereby the relevant requirements address current gaps in financial services law, and remove existing overlaps and duplications to alleviate costs. It is essential to harmonise the ICT-related incident reporting regime by requiring all financial entities to report to their competent authorities through a single streamlined framework as set out in this Regulation.[...]"

The financial entities call for legal clarity in relation to how to apply CRA incidents reporting in conjunction with the established framework under DORA. In the financial sector, the product (the app) and the entity (the bank) are inseparable. One cannot secure the vault (DORA) without securing the lock (CRA), and DORA already regulates the lock-makers (Critical Third-Party Providers). DORA was designed specifically for the unique, systemic risks of the financial system and their ICT assets and ICT systems for their entire lifecycle.

The application of CRA incident reporting adds legal complexity and administrative compliance overhead to the financial sector just after the DORA implementation deadline. CRA incident reporting directly increases the “operational challenges in addressing risk and mitigating adverse impact of ICT incidents on their own [the financial institution] and in a coherent cost-effective way.” The addition of a new taxonomy and thresholds to the financial sector is unnecessary and does not enhance the cyber resilience of financial entities or the protection of their customers. As per the Draghi report, the EU is over-regulating its financial sector compared to the US/UK.

To achieve meaningful simplification, the Digital Omnibus proposal should consider additional amendments to ensure that reporting under DORA is accepted as also covering reporting obligations under the CRA to avoid duplication of effort. The aim for the Digital Omnibus package towards simplification is maintained.

Am n°	Article	Text proposed by the Commission	Amendment proposed
	8	Article 19 of Regulation (EU) 2022/2554 is amended as follows: 1. in paragraph 1, the first subparagraph is replaced by the following: ‘Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 in accordance with paragraph 4 of this Article.’ 2. in paragraph 2, the first subparagraph is replaced by the following: ‘Financial entities may, on a voluntary basis, notify via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial	“3. in paragraph 1, the following subparagraph is added: ‘When financial entities report major ICT-related incidents pursuant to Article 19(1), such reporting shall fulfil reporting requirements under Article 14(3) of Regulation (EU) 2024/2847.’

		system, service users or clients. The relevant competent authority may provide such information to other relevant authorities referred to in paragraph 6.'	
--	--	--	--

Am n°	Recital	Text proposed by the Commission	Amendment proposed
	New 54a		(xx) In line with the principle of administrative simplification and the 'report-once' policy, it is necessary to avoid duplicative reporting obligations for financial entities that are already subject to stringent operational resilience requirements. Where a financial entity submits an incident report under Regulation (EU) 2022/2554 [DORA], that submission should be considered sufficient to satisfy the reporting requirements under the Regulation (EU) 2024/2847 [CRA]. This approach ensures regulatory coherence, legal clarity and reduces the compliance burden on the financial sector.

For more information:

Alexandra Maniati

Senior Director - Innovation & Cybersecurity
a.maniati@ebf.eu

Ingrida Taurina

Senior Policy Adviser - Innovation & Cybersecurity
i.taurina@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 33 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people.
www.ebf.eu @EBFeu