Position Paper

Euralarm Position Paper on the Implementation Timeline of the Cyber Resilience Act – 22 April 2026

1. Context and Objective

Regulation (EU) 2024/2847 establishes:

- Incident and actively exploited vulnerability reporting obligations applicable as of September 2026, and
- Essential requirements in Annex I (intended to be supported by harmonised standards) currently expected to apply from December 2027.

While the substance and ambition of these obligations are supported, the current timeline presents structural implementation gaps that risk undermining the effectiveness and coherence of the Regulation.

There is therefore a call for:

- The **adoption of a formal "stop-the-clock" mechanism** postponing the application of the reporting obligations currently set to apply from September 2026;
- A **corresponding extension of the deadline for compliance with essential cybersecurity requirements in Annex I currently foreseen for December 2027**;
- Alignment of this approach with the regulatory adjustments currently being discussed under the AI Act within the Digital Omnibus framework.

This request is aimed at ensuring effective, coherent and legally certain implementation—not at weakening cybersecurity objectives.

In addition, the Comision has recently published the Commission Delegated regulation of 16.2.2026 repealing Delegated Regulation 2022/30 which sets that *"Delegated Regulation (EU) 2022/30 is repealed with effect from 11 December 2027"*. In case that the application of certain obligations under Regulation (EU) 2024/2847 are put on hold due to the unavailability of the necessary harmonised standards and related procedures, corresponding adjustments will also be required to the Commission Delegated Regulation of 16 February 2026. Therefore, the provision stating that "*Delegated Regulation (EU) 2022/30 is repealed with effect from 11 December 2027*" should be amended to clarify that **the repeal will take effect only once Regulation (EU) 2024/2847** effectively becomes fully applicable. This alignment is essential to avoid regulatory gaps, ensure legal certainty, and guarantee a smooth and coherent transition between the existing and the new legal frameworks.

2. Why a Stop-the-Clock is Necessary?

2.1 Absence of Operational Guidance

The need for postponement is urgent and compelling. To date, there is:

- No information on reporting channels or interfaces;
- No procedural guidance or templates;
- No clarification on format or content requirements;
- No operational framework defining coordination between ENISA and national authorities.

ENISA—the entity expected to operationalise the reporting system—has not yet published implementing procedures or technical specifications. Economic operators are therefore facing binding reporting deadlines based solely on high-level provisions contained in Regulation (EU) 2024/2847, without the practical tools necessary to comply.

Introducing reporting obligations in this context creates legal uncertainty and risks inconsistent implementation across Member States. Manufacturers need this operational guidance and access to the platform for trial purposes at least 3 months before the applicability date of the reporting obligations.

2.2 Limited Readiness of National CSIRTs

The CRA reporting framework interacts with national CSIRTs (Computer Security Incident Response Teams)—public authorities responsible for receiving incident reports, coordinating response measures and facilitating cybersecurity information exchange.

In several Member States, CSIRTs are still being strengthened or reorganised following the implementation of NIS2. Their operational maturity, resources and procedures vary considerably. Introducing mandatory reporting before this infrastructure is fully stabilised risks:

- Administrative bottlenecks,
- Legal uncertainty for manufacturers and operators.

2.3 Need for availability of horizontal harmonised standards 1 year before applicability

The current deadline foreseen for December 2027 concerning the applicability of the broader cybersecurity requirements should be revised. These obligations should:

- Allow sufficient time for industry adaptation;
- Ensure consistent implementation across Member States;
- Avoid regulatory fragmentation and subsequent corrective amendments.

The Euralarm recommendation is to apply the essential requirements on products not earlier than one year after the publication of the horizontal harmonised standards prepared by CEN/CLC/JTC 13 (i.e. PT2 standard on Generic Security Requirements). This approach would align legal enforceability with the actual availability of the technical standards on which compliance depends.

3. Legal and Political Precedent

A stop-the-clock mechanism would be fully consistent with recent EU legislative practice. In April 2025, the EU adopted a so-called "Stop-the-clock" Directive, postponing the application and transposition deadlines of certain corporate sustainability reporting and due diligence requirements—even in cases where transposition had already begun in some Member States.

In contrast,

- The CRA reporting obligations have not yet entered into application;
- The CRA is a Regulation, directly applicable, rather than a Directive requiring transposition.

From a procedural and legal standpoint, adopting a stop-the-clock for the CRA would therefore be comparatively more straightforward.

Furthermore, discussions within the Digital Omnibus package concerning the AI Act already reflect recognition that calibrated timeline adjustments may be necessary to ensure legal certainty and effective implementation. In the case of the CRA, the need for postponement is even more pressing, given the complete absence of operational reporting

guidance.

4. Conclusions

In light of the structural implementation gaps identified above, Euralarm calls for targeted and proportionate legislative adjustments to Regulation (EU) 2024/2847 (Cyber Resilience Act) and to the Commission Delegated Regulation of 16 February 2026 repealing Delegated Regulation (EU) 2022/30.

These adjustments are necessary to ensure legal certainty, regulatory coherence and effective implementation, while fully preserving the cybersecurity objectives of the Regulation.

Specifically, we propose:

1. **Amendment of Article 71 of Regulation (EU) 2024/2847 regarding reporting obligations**

   The reporting obligations currently scheduled to apply from 11 September 2026 should be postponed. They should instead apply **not earlier than three months after**:

   - The reporting platform and technical interfaces are formally established and operational;
   - ENISA has adopted and published the necessary procedural guidance;
   - Harmonised formats, templates and coordination mechanisms with national authorities are clearly defined.

   This adjustment would ensure that economic operators are not subject to binding legal obligations in the absence of the practical and technical means required to comply.

2. **Amendment of Article 71 of Regulation (EU) 2024/2847 regarding the applicability of essential cybersecurity requirements and intended to be supported by harmonised standards**

   The Euralarm recommendation is to apply the essential requirements on products **not earlier than one year after the publication of the horizontal harmonised standards prepared by CEN/CLC/JTC 13,**

3. **Modification of the Commission Delegated Regulation of 16 February 2026 repealing Delegated Regulation (EU) 2022/30**

   The Commission Delegated Regulation of 16 February 2026 currently provides that "*Delegated Regulation (EU) 2022/30 is repealed with effect from 11 December 2027*."

   In order to prevent regulatory gaps and ensure a smooth legal transition, this provision should be amended so that **Delegated Regulation (EU) 2022/30 is repealed only once Regulation (EU) 2024/2847 becomes fully applicable,** in accordance with the adjusted timelines requested under points 1 and 2 above.

   This alignment is essential to:

   - Avoid a situation where the existing framework is repealed before the new regime is operational;
   - Guarantee continuity of cybersecurity requirements;
   - Preserve legal certainty for manufacturers, notified bodies and market surveillance authorities.

These proposed modifications do not seek to dilute the objectives of the Cyber Resilience Act. On the contrary, they aim to ensure that its implementation is coherent, operationally feasible and legally sound, thereby strengthening its effectiveness and credibility across the Union.

About Euralarm

Euralarm represents the fire safety and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our members make society safer and secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres. Founded in 1970, Euralarm represents over 5000 companies within the fire safety and security industry valued at 67 billion Euros. Euralarm members are national associations and individual companies from across Europe.

DISCLAIMER

Gubelstrasse 11 • CH-6300 Zug • Switzerland
E: secretariat@euralarm.org
W: www.euralarm.org