



Joint industry statement call on cybersecurity & Machinery Regulation

IMAGE SOURCE: CECE

Joint industry statement call on cybersecurity & Machinery Regulation

21 January 2026 by CECE

- Industry stakeholders urge the European Commission to delay cybersecurity requirements in the Machinery Regulation until harmonised standards are available.
- Current cybersecurity provisions lack clarity and are not aligned with the Cyber Resilience Act, risking duplicated compliance and increased costs.
- SMEs face significant operational and financial challenges under the current timeline.

- **The industry requests alignment of cybersecurity rules with the CRA deadline in December 2027 to ensure legal certainty and streamlined implementation across the EU.**

Industry stakeholders call on the European Commission to postpone the application of cybersecurity provisions in the Machinery Regulation (EU) 2023/1230 and align them with the Cyber Resilience Act (CRA).

Why this matters:

- Key cybersecurity requirements (EHSR 1.1.9 and 1.2.1(f)) lack clarity and harmonised standards
- Relevant standards are not expected until late 2026, leaving insufficient time for implementation
- Misalignment with the CRA risks double compliance cycles, major cost increases and market distortion
- Manufacturers – especially SMEs – face disproportionate operational and financial burdens

We ask to align the application of these cybersecurity requirements with the CRA timeline (11 December 2027) to ensure legal certainty, avoid duplication and enable effective, harmonised implementation across the EU. This request for alignment is fully in line with the Commission's broader agenda to simplify EU rules, avoid overlapping obligations and ensure coherent implementation for businesses.

A coordinated approach will strengthen cybersecurity without compromising innovation, competitiveness or safety.

Source: CECE