Request for postponement of the application of cybersecurity provisions in the Machinery Regulation (EU) 2023/1230

The Machinery Regulation (EU) 2023/1230 will come into effect on 20 January 2027, repealing the current Machinery Directive (2006/42/EC).

While the previous revision of the machinery legislation did not introduce any radical changes, this latest revision is of a completely different order as it introduces provisions to address the risks posed by certain technologies, such as product connectivity.

There is concern within the industry that some essential health and safety requirements (EHSRs) may be interpreted and applied differently, due to their requirement to align with other new regulations, such as Regulations 2024/2847 on horizontal cybersecurity requirements (CRA). The following points in the Machinery Regulation (MR) are of particular concern:

- EHSR 1.1.9 Protection against corruption
- EHSR 1.2.1 (f) Safety and reliability of control systems

In terms of **cybersecurity requirements**, the state-of-the-art is still under development despite the existence of international standards that are known and mastered by companies to varying degrees, depending on their size. Furthermore, the future harmonised standards are not expected to be published until late 2026. This leaves manufacturers with insufficient time to adapt to the new requirements (EHSR 1.1.9 and 1.2.1).

These future harmonised standards also remain very general regarding EHSR 1.2.1 f) concerning the activation of the data log (this requirement should meet the expectations of market surveillance authorities; however, manufacturers currently have no information to help them understand these expectations).

The lack of clarity around these new requirements will lead to different interpretations and expectations among economic operators – as well as Market Surveillance Authorities and Notified Bodies - which will make it very difficult for the industry to select appropriate technologies. This will result in major market distortions and different levels of safety across the EU. **Active work on the application guide for the Machinery Regulation is crucial** in this regard. Unfortunately, the late start and subsequent lack of a reliable, harmonised European interpretation will, in practice, jeopardise smooth product development cycles.

Ultimately, the cybersecurity risks that must be addressed under the MR will also have to comply with the CRA requirements as confirmed by both DG GROW and DG CNECT. The CRA comes into effect less than 11 months after the MR becomes applicable. Avoiding a two-step approach would reduce the burden on manufacturers when allowing them to concentrate their resources on meeting CRA requirements and with that also meeting the MR requirements. **Aligning the timelines for requirements 1.1.9 and 1.2.1(f) of the MR with those of the CRA would eliminate unnecessary duplication of efforts and facilitate implementation**: Manufacturers would benefit from reduced complexity, lower costs, and streamlined certification processes.

Evidence from co-signatories' members shows that misalignment between MR and CRA would impose disproportionate burdens on manufacturers.

Co-signatories' members estimations show that compliance costs reach more than €1 million per platform architecture (the number of platform architectures may vary depending on the range of the products offered by a company). This figure covers mapping of applicable standards (€20k), training (€30k), gap analysis (€20k), risk analysis (€60k), and multiple revisions (€1.2m for six full-time staff over two years). Each Product with Digital Elements (PDE) integrated into machinery (often more than 100 per configuration) requires a Software Bill of Materials (SBOM), vulnerability management, and validation of secure updates. These tasks multiply exponentially if manufacturers are forced into a double compliance cycle, first under the Machinery Regulation (MR) and then under the Cyber Resilience Act (CRA).

The situation is even more acute for certain manufacturers where duplication of safety and cybersecurity requirements is estimated to generate €5 million in additional costs. This includes project management, documentation, software design, and double validation (€250k) and industrialisation (€300k) across potentially up to 30 machine ranges. Importantly, 70% of these costs are generic and unavoidable.

Moreover, these figures highlight that **misalignment has financial and operational consequences.**: scarce cyber skills in the job market, fragmented standards, and supply chain disruptions make double compliance cycles unmanageable.

Aligning MR cybersecurity provisions with the CRA would eliminate duplication and reduce costs. It would also allow sufficient time for the recruitment or training of experts, especially for SMEs. Postponement to December 2027 is therefore essential to ensure harmonised, efficient, and competitive implementation.

Conclusion

We urge the Commission to postpone the application of the above requirements and dispositions in Regulation (EU) 2023/1230, to allow manufacturers time to adapt their processes. This request is also in line with the European Commission's Omnibus package for greater simplification and alignment.

We therefore ask that the date on which the aforementioned cybersecurity requirements come into effect, be aligned with that of the CRA (i.e. 11 December 2027).

Co- Signatories: