September 2025

Request for postponement of the application of cybersecurity and AI-related 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 and artificial intelligence.

There is concern within the industry that certain provisions and 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) and 2024/1689 laying down harmonised rules on artificial intelligence (AIA). The following points in the Machinery Regulation (MR) are of particular concern:

- Interpretation of the notion of AI system mentioned in Annex I, Part A, items 5 and 6 referring to "safety components with fully or partially self-evolving behaviour using machine-learning approaches ensuring safety functions"

- EHSR 1.1.9 Protection against corruption

- EHSR 1.2.1 (f) Safety and reliability of control systems

With regards to the **inclusion of Artificial Intelligence notion in the MR**, the functional safety of a machine relates to the deeper layers of its architecture. Consequently, discrepancies in the understanding of products in scope of a specific conformity assessment procedures can significantly impact the design and selection of architectures, particularly when software is involved.

Furthermore, as part of the implementation of the AI Act, the European Commission has recently launched a **targeted stakeholder's consultation on High-risk AI systems**, the outcome of this consultation is likely to affect products covered by Annex I, Part A of the Machinery Regulation, creating additional uncertainty.

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 (f)).

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.

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), and that the conformity assessment procedures requirements concerning AI systems (items 5 and 6 of Annex I, Part A of the Machinery Regulation) be postponed by at least 24 months after the interpretative work on this matter has been finalised in the application guide

Co- Signatories: