

SIMPLIFICATION PRIORITIES FOR THE DIGITAL OMNIBUS

CECIMO POSITION PAPER

October 2025

CECIMO, the European Association of Manufacturing Technologies, strongly supports the European Commission's efforts to build a more coherent and innovation-friendly digital regulatory environment.

The forthcoming Digital Omnibus is both imperative and eagerly anticipated by the manufacturing sector, given the growing importance of regulating cybersecurity, data sharing, and artificial intelligence (AI), as well as the increasing compliance challenges manufacturers are facing.

Regulatory clarity and proportionality are not only essential for compliance, but they are also key enablers of innovation, productivity, and sustainable growth for Europe's machinery industry. However, the overlapping scopes and inconsistent application of the Data Act, AI Act, and Cyber Resilience Act (CRA) have created considerable legal uncertainty, particularly for machinery manufacturers and OEMs operating in complex contractual and technical environments. The Digital Omnibus should therefore deliver practical simplifications that make it easier for businesses to operate efficiently across the Single Market. CECIMO welcomes the Commission's ambition for a more business-friendly digital framework.

When different legal acts are not properly aligned, "regulatory peaks" can emerge, situations where overlapping or conflicting obligations place an uneven burden on companies. Multiple laws may regulate the same issues in different ways or rely on inconsistent definitions, forcing manufacturers to design products according to several, sometimes incompatible, specifications. In some cases, different acts even require separate reporting channels for the same safety incident. The result is more bureaucracy, higher costs, and slower innovation.

SIMPLIFICATION PRIORITIES ON CYBER RESILIENCE ACT (CRA)



1. Introduce a phased-in transition for integrators

CECIMO calls for a clear distinction between original developers of components, which under the CRA may be considered Products with Digital Elements (PDEs), and integrators who embed these components into machinery. The manufacturing industry fully supports the objective of improving cybersecurity across industrial systems and is committed to implement it, yet integrators require additional time to comply due to the complexity of supply chains.

Machine tools typically integrate numerous components sourced from various suppliers. Manufacturers can only begin compliance once these components themselves are CRA-compliant. As many component suppliers will need until 2027 to meet CRA requirements, integrators will be left with very limited time to adapt. Assembling, validating, and testing machinery often takes between 12 and 24 months, meaning that without a phased approach, compliance would be unrealistic and overly burdensome.

CECIMO, therefore, calls on the Commission to:

Grant an additional two-year transition period for integrators, ensuring a realistic implementation schedule that does not disrupt production and innovation cycles.

2. Simplify cybersecurity incident reporting obligations

CECIMO calls for the removal of duplicate cybersecurity incident reporting obligations arising from misalignment between the CRA and the NIS2 Directive. Parallel reporting requirements create unnecessary administrative burdens, legal uncertainty, and delays in incident response. When a cybersecurity incident affects both connected products and network systems, companies often have to notify multiple authorities using different platforms, templates, and procedures, frequently submitting the same information several times.

Current inconsistencies between the two legislations further complicate implementation. The terms “significant incidents” (NIS2) and “serious incidents” (CRA) differ despite addressing comparable risks. Reporting thresholds, timelines, and authorities also vary. Additionally, diverging national implementations of NIS2, for instance the inclusion of additional sectors, differing deadlines, or non-aligned audit systems, create an uneven regulatory landscape.

A fragmented reporting system weakens Europe’s overall cybersecurity framework and diverts resources from incident management to bureaucracy. The proposed one-stop-shop reporting platform would enable manufacturers to submit a single report that is automatically forwarded to the relevant national authorities, with ENISA acting solely as a technical intermediary. This system should also support secure follow-up communication between Competent Authorities, reducing redundant requests and ensuring consistency.

CECIMO, therefore, calls on the European Commission to:

Harmonise incident reporting obligations through a “one-stop-shop” reporting platform under Article 16 of the CRA, in close cooperation with ENISA and national CSIRTs, creating a single EU-level mechanism. Ensure that reporting through this platform automatically fulfils obligations under the CRA, NIS2, and GDPR.

Align the NIS2 implementation across Member States, ensuring that audit systems are mutually recognised and reporting deadlines are consistent. Aligning these frameworks would strengthen governance, reduce administrative burden, and allow manufacturers to focus on prevention, mitigation, and recovery.

3. Align cybersecurity requirements of the Machinery Regulation with the CRA

Both the Machinery Regulation (MR) and the Cyber Resilience Act introduce cybersecurity provisions for machinery. However, the CRA will take effect less than a year after the MR, creating overlapping and potentially conflicting compliance obligations. Manufacturers would first have to meet the MR cybersecurity provisions, notably EHSR 1.1.9 (Protection against corruption) and EHSR 1.2.1 (Safety and reliability of control systems) and then adapt again for the CRA, which is a duplicative and burdensome process.

Furthermore, the relevant harmonised standards underpinning these requirements are unlikely to be published before late 2026, leaving insufficient time for manufacturers to adapt their designs and processes before the MR's application date in January 2027. As previously noted, misaligned implementation timelines risk forcing companies to re-assess products twice within a short period, increasing costs and complexity. If manufacturers first implement MR-cyber requirements and then have to redo everything for the CRA, this would mean double work, more audits, more revalidation and additional documentation.

CECIMO, therefore, recommends to:

Postpone implementing cybersecurity provisions in the Machinery Regulation until the CRA requirements and the related harmonised standards are finalised and published, ideally aligning with December 2027. This ensures coherence, avoids duplication, and gives industry sufficient time and clarity to implement effective cybersecurity solutions.

SIMPLIFICATION PRIORITIES ON ARTIFICIAL INTELLIGENCE ACT



1. Delay the application of High-Risk AI system requirements

Harmonised standards for the conformity assessment of high-risk AI systems are still under development and are unlikely to be available before the end of 2026. Without these standards, manufacturers face legal uncertainty and limited time to assess impacts, adapt products and processes, and train personnel. In addition, implementation guidelines are still pending, leaving companies with unsure of how to comply or even whether they fall within the high-risk scope.

CECIMO, therefore, urges the European Commission to:

Delay the application of high-risk AI requirements by 24 months to ensure companies have enough time to adopt and incorporate harmonised standards once they are published.

Suspend the enforcement of fines until those standards and guidance documents are available, to avoid unnecessary administrative burden and to safeguard competitiveness.

2. Clarify roles and responsibilities

Under the AI Act, a “provider” is defined as the person or company that places an AI system on the market under their own name or trademark or develops it for their own use (Article 3(3)). In practice, this means that a machinery manufacturer integrating an AI module, for example, into a CNC machine and selling it under their brand becomes the “provider,” even if the AI system was developed by a third party. This creates practical challenges, as manufacturers may be held responsible for compliance requirements such as risk management or data governance without having access to key information about how the AI system was designed, trained, or maintained.

CECIMO, therefore, urges the European Commission to:

Make a clear distinction between developers, who design and train AI systems, and integrators or component suppliers, who embed these systems into machinery, ensuring that regulatory responsibilities reflect their different roles.

Ensure that original developers retain post-market obligations, such as monitoring, incident reporting, and software updates, recognising that integrators depend on their technical support.

Such clarification would bring fairness, transparency, and predictability to compliance responsibilities, ensuring a balanced and effective implementation across Europe’s industrial AI ecosystems.

3. Align the AI Act with the Machinery Regulation

As outlined above, overlaps between horizontal legislation (AI Act, Data Act, CRA) and sector-specific product law (Machinery Regulation) may create legal uncertainty and duplicate conformity assessments. Divergent definitions, such as “safety component”, further complicate compliance.

The inclusion of AI-related provisions in the Machinery Regulation introduces uncertainty for manufacturers. References to “safety components with fully or partially self-evolving behaviour using machine-learning approaches ensuring safety functions” in Annex I, Part A, items 5 and 6, directly link the MR to the evolving framework of the AI Act. However, the definitions and classifications of “high-risk AI systems” are still under consultation, and harmonised standards are not yet available. This situation affects how manufacturers design and assess AI-enabled safety components and control systems, particularly in relation to functional safety, validation, and software architecture.

CECIMO, therefore, recommends to:

Postpone the conformity-assessment requirements for AI-based safety components and machinery in the Machinery Regulation by at least 24 months, until the MR Application Guide has finalised its interpretation and the scope of the AI Act is clearly defined.

This postponement would allow alignment with the final provisions of the AI Act and the publication of harmonised guidance, ensuring consistent interpretation, legal certainty, and fair market conditions across the EU. This would give industry the necessary time to integrate harmonised standards and guidance effectively, enabling manufacturers to design and comply their products once and correctly.

SIMPLIFICATION PRIORITIES ON DATA ACT



1. Stop the clock on implementation

CECIMO fully supports the objectives of the EU Data Act to promote transparent, fair, and innovation-driven data sharing. However, given the sector's complex B2B value chains and extensive base of connected and legacy machines, complying within the current timeline poses serious challenges.

Machine tool manufacturers often operate through distributors and integrators without direct contractual relationships with end users, making compliance with new data-sharing obligations particularly difficult. Identifying thousands of users of existing machines and negotiating or amending data-sharing contracts is both administratively and legally demanding. Moreover, many machines predate connectivity requirements, adding layers of technical and contractual complexity.

CECIMO, therefore, calls on the European Commission to:

Adopt a one-year “stop-the-clock” period, postponing the application of Chapters 2, 3, and 4 of the Data Act to 12 September 2026.

This would allow companies to renegotiate contracts, identify end users, and integrate forthcoming Model Contractual Terms and guidance on reasonable compensation, expected shortly before the current deadline. Without this period, manufacturers risk fragmented or non-compliant agreements that undermine legal certainty and Single Market consistency. It would also give companies time to adapt technical and cybersecurity protocols, ensuring data sharing does not compromise machine integrity, intellectual property, or safety-critical functions. For the machine tool sector, which supports production across nearly every industrial value chain, correct implementation of the Data Act is essential to maintain Europe's competitiveness and ensure data sharing strengthens, rather than disrupts, the manufacturing ecosystem.

2. Protecting trade secrets in data sharing


Trade secrets must be explicitly excluded from mandatory data-sharing obligations in B2B contexts, including access requests by third parties. Current provisions provide insufficient protection for trade secrets in B2B data-access scenarios, creating legal uncertainty and undermining Europe's technological sovereignty objectives.

B2B industrial systems have very different risk profiles from consumer products. Their long-life cycles, integration with legacy systems, and complex contractual risk-sharing arrangements demand a more tailored approach to data access and protection, ensuring that industrial know-how remains secure while still enabling fair and responsible data sharing.

FOR MORE INFORMATION, PLEASE CONTACT:

Olha HUNCHAK

Digital and Technical Policy Manager

 olha.hunchak@cecimo.eu

About CECIMO:

CECIMO is the European Association of Manufacturing Technologies. With a primary focus on machine tools and additive manufacturing technologies, we bring together 15 national associations representing approximately 1500 industrial enterprises in Europe (EU + UK+ EFTA + Türkiye), over 80% of which are SMEs. CECIMO covers 97% of the total machine tool production in Europe and about 1/3 worldwide. It accounts for approximately 150,000 employees and a turnover of around 25.8 billion euros in 2024.

CECIMO Members



Austria: Metaltechnology Austria
Die MetalltechnischeIndustrie



Germany: VDW
Verein Deutscher
Werkzeugmaschinenfabriken e.V.



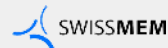
Sweden: MTAS
Machine and Tool Association of Sweden



Belgium: AGORIA
The Federation of Technology Industry



Italy: UCIMU
Associazione dei costruttori Italiani di macchine utensili
robot e automazione



Switzerland: SWISSMEM
Die Schweizer Maschinen-, Elektro- und Metall-
Industrie



Czech Republic: SST
Svazu Strojírenské Technologie



Netherlands: FPT-VIMAG
FederatieProductieTechnologie / Sectie VIMAG



Türkiye: MIB Makina
İmalatçıları Birliği



Denmark: The Manufacturing Industry
a part of the Confederation of Danish Industry



Portugal: AIMMAP
Associação dos Industriais Metalúrgicos,
Metalomecânicos e Afins de Portugal



United Kingdom: MTA
The Manufacturing Technologies Association



Finland: Technology Industries of Finland



Spain: AFM Cluster
Asociación española de fabricantes de máquinas-
herramienta, accesorios, componentes y herramientas



France: Evolis
Organisation professionnelle des biens
d'équipement