cecimo
European Association of Manufacturing Technologies

CECIMO'S POSITION ON PROPORTIONATE IMPLEMENTATION OF THE CRA

CECIMO POSITION PAPER

November 2026



CECIMO, the European Association of Manufacturing Technologies, welcomes the Commission's Guidance on the application of Regulation (EU) 2024/2847, the Cyber Resilience Act (CRA). The Guidance provides useful clarification on several issues previously raised by the industry, including support periods, substantial modifications and the scope of the regulation. In particular, CECIMO welcomes the clarification that routine maintenance, repairs and cybersecurity updates do not automatically constitute substantial modifications, as well as the recognition of a proportionate approach to conformity reassessment.

CECIMO fully supports the CRA's objective of strengthening cybersecurity across the EU market. At the same time, its implementation should reflect the specific characteristics of industrial machinery, particularly its long operational lifetime and the need for continuous maintenance and modernisation. Building on the Commission's Guidance, CECIMO has identified four areas where further clarification and a proportionate approach could help manufacturers meet their obligations while avoiding unnecessary complexity and costs: substantial modifications; the application of cybersecurity requirements at component level; support periods for long-life machinery; and practical technical guidance and standardisation.

1. Substantial Modifications under Article 22 of the CRA

Machine tools are designed to operate for decades and are regularly maintained, upgraded and modernised throughout their lifetime. Such interventions may involve replacing components, introducing new software functions or enhancing cybersecurity measures. However, treating substantial modifications as a newly placed on the market could trigger additional conformity assessment obligations, potentially complicating and increasing the cost of modernising existing machinery. This could discourage manufacturers from upgrading otherwise functional equipment, which would undermine the longevity and sustainability of European machine tools.

Article 22(1) of the CRA explicitly distinguishes between original manufacturers and other parties carrying out substantial modifications. Under this provision, any party other than the original manufacturer, importer or distributor that substantially modifies a product and makes it available on the market is considered a manufacturer for the purposes of the Regulation. However, the Commission's Guidance states that a substantially modified product made available on the market is considered newly placed on the market even when the modification is carried out by the original manufacturer.

CECIMO is concerned that this interpretation could impose disproportionate requirements on original manufacturers modernising machinery already in service, particularly through software upgrades and retrofits involving interconnected systems. Original manufacturers remain responsible for their applicable CRA obligations, including handling vulnerabilities during the relevant support period. Excluding them from the specific legal consequences of Article 22 therefore does not remove their existing cybersecurity responsibilities. While the Guidance recognises a proportionate approach to reassessment, including the reuse of existing conformity evidence, it does not fully address the implications of treating substantially modified machinery as newly placed on the market.

These implications may extend beyond the CRA, as modifications to existing machinery may also need to be assessed under the Machinery Regulation and other applicable EU product legislation. The differences in how these frameworks define and assess substantial modifications, and in their legal consequences, can create uncertainty about when new conformity assessments are required and lead to overlapping compliance requirements, potentially making the modernisation of older machinery technically or economically impractical.

CECIMO therefore calls on the Commission to reconsider the relevant parts of its Guidance, ensuring that the explicit distinction established by Article 22 is properly reflected in its interpretation of when substantial modifications carried out by original manufacturers result in a new placing on the market. More broadly, CECIMO calls for closer coordination across EU product legislation, including the Machinery Regulation, to ensure greater consistency in determining when substantial modifications trigger new conformity assessment obligations, while respecting the specific requirements of each framework. A pragmatic and proportionate approach to the interpretation of substantial modification would help reduce legal uncertainty and avoid unnecessary compliance burdens, encouraging manufacturers to continue modernising long-life industrial machinery without compromising cybersecurity or safety.

2. Proportionate Application of CRA Requirements At Component Level

CECIMO is also concerned that certain parts of the Commission's Guidance may interpret the flexibility provided by the CRA too narrowly when determining which cybersecurity requirements apply to industrial components. This could lead to disproportionate requirements at component level, potentially increasing costs and limiting the availability of components for machine manufacturers.

Article 13 requires manufacturers to assess and document the cybersecurity risks of a product and determine how the relevant essential cybersecurity requirements apply in light of its intended purpose and reasonably foreseeable use. Where a specific requirement is considered inapplicable, this must be justified in the technical documentation. Recital 55 further recognises that, where a related cybersecurity risk still exists, it may in certain cases be addressed through other appropriate measures, such as limiting the product's intended purpose to trusted environments or informing users about the relevant risks. The recital also acknowledges that interoperability may require the use of widely recognised standards, even where their security features do not fully reflect the latest technological advances.

The practical implications depend on how components enter the EU market. When a component is placed separately on the EU market, it must meet the applicable CRA requirements on its own. However, when a component is incorporated directly into a finished machine without being separately placed on the EU market, the machine manufacturer is responsible for assessing and addressing the cybersecurity risks associated with that component. In either case, the finished machine must comply with the CRA when placed on the EU market.

Section 7.1 of the Commission's Guidance explains that commercial considerations or manufacturers' internal risk tolerance cannot justify leaving cybersecurity risks unaddressed, nor can responsibility simply be transferred to users or third parties. While these principles are understandable, CECIMO considers that the guidance should not unduly restrict the flexibility recognised in Recital 55 and Article 13, particularly for industrial components whose intended purpose, operating environment or interoperability requirements may justify different approaches to addressing cybersecurity risks.

CECIMO therefore calls on the Commission to clarify in its Guidance the application of Article 13(4) and Recital 55, ensuring that manufacturers can assess and justify the applicability of cybersecurity requirements based on the intended purpose, operating environment, reasonably foreseeable use and associated cybersecurity risks, and adopt appropriate alternative measures where justified. Further clarification is also needed on the information and cooperation required between component suppliers and machine manufacturers, particularly regarding vulnerability reporting, security updates and relevant technical information. This would preserve the CRA's risk-based approach, avoid unnecessary compliance burdens and support coordinated implementation across the supply chain without compromising cybersecurity protection.

3. Support Period for Long-Life Machinery and Integrated Components

Machine tools are designed to operate for decades, whereas critical third-party digital components, such as control systems, may have significantly shorter support periods. This presents challenges for machine manufacturers, as they remain responsible for effectively handling vulnerabilities throughout the support period of the finished machine, even when security updates or technical support depend on component suppliers. Once supplier support expires, manufacturers may need to implement alternative security measures or replace affected components. This can increase lifecycle costs, particularly for SMEs that might have limited access to suitable replacement components or the technical means to address vulnerabilities independently.

Article 13(8) of the CRA requires manufacturers to determine a support period that reflects the expected use of their products and to ensure effective vulnerability management throughout that period, including for integrated components. The Regulation allows manufacturers to take into account the support periods of third-party components providing core functions, alongside other relevant factors, in a proportionate manner. While the Commission's FAQs already clarify manufacturers' continuing responsibilities when component support expires, further practical guidance would help address the specific challenges of long-life industrial machinery.

A related challenge concerns components held in stock before being integrated into new machinery. If components remain in stock for an extended period, part of their supplier's support period may have elapsed by the time they are integrated. Their remaining support may therefore be considerably shorter than the expected support period of the finished machine, creating uncertainty about how such components should be assessed before integration and how manufacturers should manage the resulting cybersecurity obligations.

CECIMO therefore calls on the Commission to provide further practical clarification in its Guidance and FAQs on how manufacturers should manage differences between the support periods of long-life industrial machinery and its integrated components. In particular, greater clarity is needed on the vulnerability information, security updates, technical support, end-of-support notices and replacement options that component suppliers can reasonably be expected to provide. It should also address what can reasonably be expected from machine manufacturers when supplier support expires, particularly where they lack the technical information, access rights or practical means to address vulnerabilities independently.

This includes how to assess whether measures such as component replacement, isolation or other compensating security measures are appropriate and sufficient to address identified vulnerabilities, and when updated operating instructions may be needed to support these measures. Further clarification is needed on how manufacturers should assess and manage components whose support periods have already partly elapsed before integration into new machinery. Together, these clarifications would provide greater legal certainty and support proportionate vulnerability handling, particularly for SMEs, while maintaining the CRA's cybersecurity objectives.

4. Practical Technical Guidance and Standardisation

Beyond the specific issues outlined above, CECIMO believes that more practical and technical clarity is needed to support the consistent implementation of the CRA, especially for SMEs. While the Commission's Guidance and FAQs already provide valuable clarifications and practical examples, uncertainty about translating legal requirements into concrete technical measures could lead to unnecessary compliance costs and differing interpretations among manufacturers.

CECIMO therefore encourages the Commission to continue supporting the timely development and citation of relevant harmonised standards and, complemented where necessary by practical guidance tailored to industrial machinery. Concrete examples would be particularly valuable for cybersecurity risk assessment, vulnerability handling and technical documentation, including asset inventories and software bills of materials (SBOMs). They could help manufacturers determine whether known vulnerabilities affect the finished machine, understand interactions between machine systems and software updates, and clarify the role of professional users in maintaining cybersecurity.

Particular attention is also needed to the practical constraints of deploying security updates in industrial machinery, including safety validation and planned maintenance windows. Where immediate deployment is not feasible, practical guidance on appropriate temporary risk-mitigation measures would help manufacturers manage vulnerabilities until updates can be safely implemented. Throughout, it is important to distinguish between mandatory CRA requirements, voluntary technical means of demonstrating compliance and recommended good practices. This would help manufacturers understand and demonstrate compliance more consistently and proportionately, while maintaining the CRA's cybersecurity objectives.

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 technologies, we bring together 14 national associations of machine tool builders, which represent 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 23.4 billion euros in 2025.

*CECIMO8 Total orders index is a combined domestic and foreign orders index of eight major CECIMO MT producers (Germany, Italy, Switzerland, Spain, Austria, France, the United Kingdom and the Czech Republic), weighted by 2021 production levels.

CECIMO Members

Austria: Metaltechnology Austria
Die MetalltechnischeIndustrie

Germany: VDW
Verein Deutscher Werkzeugmaschinenfabriken e.V.

Sweden: MTAS
MTAS – Manufacturing Technologies Association 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 Imalatcilari Birligi

Finland: Technology Industries of Finland

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

United Kingdom: MTA
The Manufacturing Technologies Association

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

France: Evolis
Organisation professionnelle des biens d'équipement