



EUROMOT

The European Association of Internal
Combustion Engine and Alternative
Powertrain Manufacturers

POSITION PAPER

Cyber Resilience Act (CRA): Applicability to Engines

10 July 2026

**CYBER
RESILIENCE
ACT**





The European Association of Internal
Combustion Engine and Alternative
Powertrain Manufacturers

EUROMOT POSITION

CYBER RESILIENCE ACT (CRA): APPLICABILITY TO ENGINES

10 JULY 2026, BRUSSELS

Executive Summary

The implementation of the EU Cyber Resilience Act (CRA) raises fundamental questions for complex, business-to-business (B2B) industrial supply chains, particularly in the nonroad mobile machinery and powertrain sectors. Legal uncertainty persists as to when engines, engine components, electronic control units (ECUs), and associated software qualify as a *product placed on the market* (POM) under the CRA, and which economic operator should bear the corresponding regulatory obligations. EUROMOT considers this clarification essential to ensure proportionate, workable, and cost-effective implementation of the CRA, while preserving the established allocation of responsibilities in industrial value chains.

1. Main question to the European Commission:

Is an engine, engine component, Electronic Control Unit (ECU), or software considered a “product with a digital element placed on the market” (POM) under the CRA, and if so, by whom?

To help answer this question, we’ve outlined different scenarios or use cases below in section 3.

The answer is essential to:

- Clarify CRA responsibilities (Declaration of conformity (DoC), CE marking...) in B2B industrial supply chains;
- Distinguish responsibilities between engine manufacturer, integrator, OEM (original equipment manufacturer) and final product manufacturer;



EUROMOT aisbl, Rue Joseph Stevens 7, 1000 Brussels, Belgium
A European Interest Representative · TVA BE 0599.830.578 · RPM Brussels
EU Transparency Register Id. No. 6284937371-73

A Non-Governmental Organisation in consultative status with the UN Economic Commission for Europe (UNECE) and the UN International Maritime Organisation (IMO)

PRESIDENT
Dr Holger Lochmann

GENERAL MANAGER
Dr Peter Scherm

- Clarify which economic operator is responsible for fulfilling CRA obligations, including technical documentation, CE marking and cybersecurity requirements;
- Ensure legal certainty and unambiguous allocation of responsibilities, compliance obligations and liability in contractual arrangements across the value chain.

2. Background and Context

Engines with a digital element, ECUs and software are typically designed for integration into larger systems or machines. Their cybersecurity risk profile, intended use, and exposure to threats are often fully determined only at the level of final integration. Applying the CRA without adequately reflecting this industrial reality risks duplicative compliance efforts, unclear liability allocation, and disproportionate regulatory burden for upstream suppliers.

To illustrate these challenges, EUROMOT sets out a (non-exhaustive) series of concrete and representative use cases where clarification is urgently needed.

3. Use Cases Requiring Clarification

3.1. Use Case 1 – Complete Vehicle Imported into the EU

Scenario

A complete agricultural tractor manufactured outside the EU arrives at an EU port. The vehicle is finished, ready for sale, and intended for immediate use.

Key Question

- Can the Commission confirm that, at this point in time, the complete vehicle qualifies as a product placed on the EU market under the Cyber Resilience Act, and that full CRA obligations therefore apply to the entity importing the complete vehicle into the EU and placing it on the market?

3.2. Use Case 2 – Complete Engine Imported Separately

Scenario

A complete Stage V internal combustion engine, including the engine block, an electronic control unit (ECU), and embedded application-specific software, is supplied on the EU market for integration into a machine by another manufacturer (OEM).

This situation covers both:

- engines imported into the EU; and
- engines manufactured within the EU and supplied on a B2B basis to machinery manufacturers exclusively for integration into final machinery.

In accordance with Directive 2006/42/EC and Regulation (EU) 2023/1230 (Machinery Regulation), such engines qualify as partly completed machinery (PCM) (quasi-machines).



EUROMOT aisbl, Rue Joseph Stevens 7, 1000 Brussels, Belgium

A European Interest Representative · TVA BE 0599.830.578 · RPM Brussels
EU Transparency Register Id. No. 6284937371-73

A Non-Governmental Organisation in consultative status with the UN Economic Commission for Europe (UNECE) and the UN International Maritime Organisation (IMO)

PRESIDENT

Dr Holger Lochmann

GENERAL MANAGER

Dr Peter Scherm

They are placed on the market accompanied by a Declaration of Incorporation, do not need Declaration of Conformity (DoC) but are not CE-marked as finished machines, as they are not intended to operate autonomously.

The engine is equipped with an ECU and embedded software that is functional and tailored to a specific OEM application. While core engine control functions are defined at engine level, the final system context in which the ECU operates, including:

- external interfaces and interactions with other components
- connectivity features and network exposure
- system architecture and configuration
- operational environment and use conditions

is determined only at the stage of integration into the final machine by the OEM.

From a cybersecurity perspective, the engine manufacturer can implement appropriate security-by-design measures at engine level. However, the engine cannot be considered fully cybersecure in isolation. The final cybersecurity risk profile depends on machine-level integration, where additional functionalities, interfaces, and exposure to cyber threats are introduced.

As a result, the overall cybersecurity posture is not solely determined by the intrinsic characteristics of the ECU or engine, but primarily by the way the product is integrated, configured, and deployed within the final machine.

At the same time, compliance with CRA essential cybersecurity requirements cannot be achieved solely at final machine level without structured contribution from upstream suppliers. In practice, the manufacturer placing the final product on the market depends on supplier-provided cybersecurity artefacts and evidence, including SBOM information, vulnerability handling inputs, cybersecurity assessments, and verification results.

This reflects a model where the final product manufacturer retains full legal responsibility, supported by necessary cybersecurity contributions and evidence from upstream suppliers.

In practice, it is therefore not realistic for the engine manufacturer to ensure full compliance with all obligations under the CRA without knowledge of the final machine configuration and operational context, which are defined by the manufacturer responsible for final integration and placing the finished product on the market.

Key Questions

- **Qualification under the CRA**

Should an engine, supplied as partly completed machinery and equipped with an ECU and embedded application-specific software, be considered a “product with digital elements placed on the market” under the CRA at the engine level?

- **Scope of obligations at component level**

To what extent can CRA obligations (including cybersecurity requirements, CE marking, technical documentation, and vulnerability handling) reasonably apply to the engine manufacturer, given that essential cybersecurity characteristics are defined only during integration at machine level?



EUROMOT aisbl, Rue Joseph Stevens 7, 1000 Brussels, Belgium

A European Interest Representative · TVA BE 0599.830.578 · RPM Brussels
EU Transparency Register Id. No. 6284937371-73

A Non-Governmental Organisation in consultative status with the UN Economic Commission for Europe (UNECE) and the UN International Maritime Organisation (IMO)

PRESIDENT

Dr Holger Lochmann

GENERAL MANAGER

Dr Peter Scherm

- **Allocation of responsibilities across the value chain**

How should CRA responsibilities be proportionately and clearly allocated between:

- the legal responsibility of the manufacturer placing the final product with digital elements on the market; and
- the technical and operational cybersecurity responsibilities of upstream suppliers (e.g. engine manufacturers and ECU suppliers), whose activities and evidence are required to enable compliance of the final product?

- **Consistency with the Machinery framework**

How can coherence be ensured between:

- the concept of partly completed machinery under the Machinery Directive/Regulation; and
- the notion of a product placed on the market under the CRA,

in order to avoid overlapping, duplicative, or disproportionate compliance obligations for upstream suppliers?

Clarification should ensure that recognising supplier cybersecurity contributions does not result in engines, ECUs, or components being treated as independent CRA products, as this would conflict with the concept of partly completed machinery and lead to duplicated conformity assessment and disproportionate regulatory burden.

- **Applicability of specific CRA requirements**

To what extent are manufacturers, importers, or authorised representatives of partly completed machinery required to comply with CRA provisions (including relevant Annexes on essential cybersecurity requirements, conformity assessment, technical documentation, and vulnerability handling)?

- **Dependency on supply chain inputs**

How should the CRA explicitly recognise the dependency of the final product manufacturer on upstream suppliers for cybersecurity artefacts and evidence — including SBOM information, vulnerability handling inputs, cybersecurity assessments, and verification evidence — without thereby classifying partly completed machinery, engines, or ECUs as independent “products with digital elements placed on the market”?

- **Conclusion (Use Case 2)**

Overall, the framework should preserve a clear distinction between legal responsibility at final product level and the distributed technical responsibilities across the supply chain that are necessary to achieve CRA compliance in practice.

3.3. Use Case 3 – Single ECU Imported as a Module

Scenario

A single ECU is imported into the EU as a hardware module, without software, intended for later integration and **not marketed as a spare part**.

Key Questions

- Does such an ECU, in isolation, constitute a product placed on the market under the CRA?
- Does CRA responsibility arise only once software is installed and the ECU becomes functionally operational within a system?

3.4. Use Case 4 – White-Labeling and Contractual Allocation of Responsibility

Scenario

A company responsible for placing a final product on the market under its own name or trademark does not have the in-house capability to develop certain components or software (e.g. an ECU, control software, or battery management system). It therefore mandates an external supplier to develop the component or software *as an engineering or technical service*. A supplier therefore develops a component (e.g. an ECU or battery) exclusively for a client.

The developed component or software is not sold, or made available independently by the supplier, nor under the supplier's name or trademark. It is developed exclusively for integration into the customer's own product.

Under this model, the supplier acts purely as a technical partner supporting development. All regulatory responsibility, including the determination of whether a product is placed on the market and the fulfilment of CRA obligations (including CE-marking where applicable), is assumed by the customer as the sole POM entity, as explicitly agreed contractually.

Internal coordination, information exchange, and cooperation between the customer and its technical partner for the purpose of meeting CRA requirements take place as part of a contractual relationship and do not constitute a separate act of placing a product on the market by the supplier.

Key Questions

- Can a supplier providing components or software purely as an engineering or development service be excluded from independent CRA obligations where it does not place any product on the market under its own name? In other words, in this scenario,
 - can the customer, as the only entity agreeing contractually to place the product on the market, be recognised as the sole POM and responsible person under the CRA?
 - can the supplier remain a technical partner only, without independent CRA obligations?
- How should the CRA distinguish between technical cooperation in product development and the act of placing a product on the market?

3.5. Use Case 5 – Software

Scenario

In industrial B2B value chains, software does not circulate in a single, standardized way: it may be embedded in hardware, supplied digitally as part of a system, updated after initial deployment, or transferred contractually between parties without independent commercialization.

This use case is intended to bring clarity on how CRA obligations should apply to software that does not follow a uniform circulation model, and on how economic operators should determine, in practice and on a case-by-case basis, whether CE marking and other CRA obligations apply.

Key Questions

- In which concrete scenarios should software be considered a product placed on the market under the CRA?
- How should CRA obligations differ where software is:
 - embedded in hardware and not independently commercialized; or
 - made available, transferred, or updated separately from hardware?
- How should economic operators determine whether and when software requires CE marking, given its non-standard circulation patterns?

4. Closing Request to the European Commission

EUROMOT respectfully calls on the European Commission to provide simple, concrete, and example-based guidance addressing the above use cases, in order to clarify:

- When engines with digital elements, components, ECUs and software qualify as products placed on the market under the CRA;
- Which economic operator bears legal responsibility and liability in complex, multi-stage B2B supply chains;
- Can CRA responsibilities be contractually allocated without creating legal and liability uncertainty or duplicative obligations.

Such clarification is essential to ensure that the CRA is implemented in a predictable, proportionate and innovation-friendly manner for the industrial engine and machinery sectors.



EUROMOT aisbl, Rue Joseph Stevens 7, 1000 Brussels, Belgium

A European Interest Representative · TVA BE 0599.830.578 · RPM Brussels
EU Transparency Register Id. No. 6284937371-73

A Non-Governmental Organisation in consultative status with the UN Economic Commission for Europe (UNECE) and the UN International Maritime Organisation (IMO)

PRESIDENT

Dr Holger Lochmann

GENERAL MANAGER

Dr Peter Scherm

THIS IS EUROMOT

EUROMOT, the European Association of Internal Combustion Engine and Alternative Powertrain Manufacturers, represents the key manufacturers of internal combustion engines and alternative powertrains installed in industrial non-road mobile machinery, marine and stationary applications that are operating in Europe and worldwide.

Founded in 1991, we provide an unparalleled heritage and hub of expertise for businesses, authorities, regulators, and public stakeholders worldwide. In partnership with major sector associations and institutions, it is our mission to drive smart regulation and sustainable innovation.

Delivering dependable power for society at high energy conversion efficiency with low emissions remains a key objective of EUROMOT member companies. EUROMOT asserts internal combustion engines and alternative powertrains are a key enabler to address the additional societal need for decarbonisation across multiple industry sectors. This can be achieved by continuing to advance the development of highly efficient energy conversion systems capable of operating on low and net-zero Greenhouse Gas (GHG) energy carriers.

Headquartered in Brussels, EUROMOT is a European interest group, and our profile is registered in the EU Transparency Register under the identification number 6284937371-73. We have been granted consultative status at the United Nations IMO (International Maritime Organization, London) and United Nations ECE (Economic Commission for Europe - Geneva) and other relevant stakeholders.

OUR MEMBERS



EUROMOT aisbl, Rue Joseph Stevens 7, 1000 Brussels, Belgium
A European Interest Representative · TVA BE 0599.830.578 · RPM Brussels
EU Transparency Register Id. No. 6284937371-73

A Non-Governmental Organisation in consultative status with the UN Economic Commission for Europe (UNECE) and the UN International Maritime Organisation (IMO)

PRESIDENT
Dr Holger Lochmann

GENERAL MANAGER
Dr Peter Scherm



Contact Us

EUROMOT aisbl

The European Association of Internal
Combustion Engine and Alternative
Powertrain Manufacturers

Aliénor Poher
Senior Manager Regulatory Affairs
and Sustainability



+32 (0) 28 93 21 42



Rue Joseph Stevens 7
1000 Brussels - Belgium



alienor.poher@euromot.eu



www.euromot.eu

TVA BE 0599.830.578

RPM Brussels

EU Transparency Register
ID number: 6284937371-73