October 2027

EVOLIS's proposals in response to the ongoing consultation on the Digital Omnibus Package.

The manufacturers represented by EVOLIS welcome the objectives of the Digital Omnibus package to simplify, align and harmonise the current regulatory landscape and EVOLIS generally supports the EU's digital transformation, enacted through various new pieces of legislation. However, this should not result in additional costs or challenges for an industry that is already under pressure.
As part of the ongoing consultation on the European Commission's proposal for the Digital Omnibus Package, the following position aims to simplify the legislative landscape, particularly regarding cybersecurity, in line with concerns raised by many French manufacturers. Thus EVOLIS strongly supports the European Commission's initiative for simplification and has identified three areas for improvement:

1- Simplification of reporting obligations for cybersecurity incidents under NIS2 and CRA;
2- Alignment of application dates for the cybersecurity requirements under Machinery Regulation and CRA;
3- Creation of the concept of "digital lifetime" under the CRA.

1 Simplification of reporting obligations for cybersecurity incidents under NIS2 and CRA.

Reporting obligations will be implemented through two main pieces of legislation: NIS2 and the CRA. However, even though the objectives are similar, the processes are not aligned, creating an unnecessary administrative burden for the manufacturing industry: The same cybersecurity incident will have to be reported twice via different channels.
The EVOLIS proposal is to revise the NIS2 Directive and align the reporting obligations with the requirements established in the CRA, covering processes, terminology, delays and actors together.

2 Alignment of application dates for the cybersecurity requirements under Machinery Regulation and CRA.

When the legislative proposal for the Machinery Regulation was published, the industry expressed strong concerns about the inclusion of new cybersecurity requirements (i.e. EHSR 1.1.9 and 1.2.1(f) of Annex III), which were perceived as posing a potential risk of overlap or misalignment with the future CRA.
Now the current situation will require manufacturers to take a staggered approach to addressing cybersecurity risks due to the different application dates (January 2027 for the

EVOLIS
45 rue Louis-Blanc 92400 Courbevoie
Siret : 785 425 810 00021 - Code Ape : 9412Z
TVA intracommunautaire : FR02 785 425 810
www.evolis.org

Machinery Regulation and December 2027 for the CRA), whereas a holistic approach to cybersecurity should cover all aspects at once (a principle reinforced by the NIS2 directive). In practice, this misalignment will lead to:

- Potential for successive hardware migrations within a short timeframe, which is not industrially viable.
- Additional updates to factory programming, testing processes, or potential physical adjustments to the hardware.

Although the industry welcomes the new cybersecurity requirements, misaligned timelines would force manufacturers to adapt these processes twice, resulting in inefficiencies and increased costs.
The EVOLIS proposal for simplification is to postpone the application of EHSR 1.1.9 and 1.2.1(f) of the Machinery Regulation until 11 December 2027, when the CRA comes into effect. This would benefit manufacturers by reducing complexity and costs, streamlining certification processes, avoiding redundant efforts, and facilitating practical implementation.

3 Creation of the concept of "*digital lifetime*" under the CRA.

The CRA's inclusion of a support period to address cybersecurity vulnerabilities is raising questions about the practical implications for manufacturers. According to the CRA, manufacturers should consider product lifetimes when determining support period lengths, which could potentially trigger obligations for products with digital elements that are no longer being sold.
Some of the products represented by EVOLIS (e.g. excavators or cranes) have a product lifetime of 20–25 years, sometimes more. However, when it comes to cybersecurity risks, the strength or durability of materials other than digital components should not be considered when defining the support period, to avoid the risk of programmed obsolescence. **EVOLIS's proposal is to add in the CRA the concept of 'digital lifetime'** determined by manufacturers, to better reflect actual cybersecurity risks and needs, without incurring disproportionate costs.

In an era of significant change, industry faces many challenges, ranging from the digital revolution to environmental transition and national sovereignty. As producers of industrial equipment, machinery, and solutions, EVOLIS members play a vital role in the industrial value chain, providing essential solutions to help major industrial sectors overcome their transformation challenges.