Customer Information
MVO/CRA

Erhardt+Leimer

Information on the Cyber Resilience Act (CRA) and the Machinery Regulation (EU) 2023/1230

Stadtbergen, 07-01-2026

Dear Sir or Madam,

We are currently receiving an increasing number of inquiries regarding the upcoming mandatory implementation of the requirements set by the EU Machinery Directive and the Cyber Resilience Act (CRA), on which we would like to comment in this letter.

We at Erhardt+Leimer GmbH are aware of the importance of the issues raised in the context of the Cyber Resilience Act (CRA) and the Machinery Regulation (EU) 2023/1230, and we are working to implement the relevant requirements within the specified deadlines.

As a supplier of components and partly completed machinery, the scope of the measures to be implemented depends on our role within the supply chain and the intended use of our products. Certain measures, particularly network-based protective mechanisms such as firewalls, fall outside the scope of our system and must be ensured by the machine manufacturer as part of the overall integration process and by the operating company during operation.

Our products already meet the essential requirements of state-of-the-art cybersecurity standards and are designed in accordance with the specifications of IEC 62443-4-2. For example, components featuring EL.NET technology include role-based access controls and logging functions. These security features are being gradually expanded to other product lines.

Since our components are typically not directly connected to public networks but can be used in networked environments, and since the decision on when to replace or modify software rests with the operator or the machine manufacturer, we will ensure that firmware and security-related updates are made available in a structured manner via appropriate portals in the future.

A process for addressing vulnerabilities and security incidents will be established and further developed in accordance with the CRA’s requirements. This includes timely reporting to the relevant authorities and notifying affected customers. In the event of known vulnerabilities or security incidents, we will proactively contact our relevant customers - as we already do today.

The principles of “security by design” and “security by default” are systematically integrated into our development processes and are currently being further expanded company-wide. In the future, software bill of materials (SBOMs) will be provided in a structured and appropriate format, and eventually in a machine-readable format as well, to ensure transparency regarding the Software components used.

Customer Information
MVO/CRA

Erhardt+Leimer

Our EL.NET components primarily utilize software solutions that we have developed in-house as well as proprietary solutions. The specific versions currently installed can already be viewed via the components' Web-Based Management (WBM) system, as well as through the system bill of materials or spare parts list that can be generated there.

We hope the information provided above has been helpful. Since the harmonization of the relevant standards has not yet been completed and regulatory requirements are still evolving, we are unable to provide any binding or further detailed information on the topics mentioned at this time. The Erhardt+Leimer GmbH website will be expanded to include a section on security, so that in future you will be able to find all the relevant information on this topic there.

Best regards,

Joachim Tatarczyk
Managing Director I Group COO

Erhardt+Leimer GmbH