We would like to share an update on EnOcean's current status regarding the EU Cyber Resilience Act (CRA – Regulation (EU) 2024/2847) and outline our roadmap toward full compliance.

On 20 November 2024, the CRA was published in the Official Journal of the EU. The CRA introduces horizontal cybersecurity requirements for all products with digital elements (hardware and software with connectivity), aiming to ensure these products are designed, developed, and maintained with a high level of cyber resilience throughout their lifecycle.

As part of our proactive approach, we have completed an internal applicability assessment of the CRA across our portfolio. This assessment has confirmed that:

- Many EnOcean products qualify as **"products with digital elements"** under the CRA.
- A classification of our portfolio under the CRA has been carried out, identifying both **default** and **important** product categories according to Annex III of the CRA. **No critical products** listed in Annex IV are identified.
- Based on this classification, our compliance activities are being tailored to the obligations applicable to each product category.

Building on Our Strong Regulatory Foundation

EnOcean is well positioned for this transition due to its strong existing regulatory and cybersecurity foundation.

- **Many of our devices are already CE marked** and conform to existing European regulatory frameworks such as the **Radio Equipment Directive (RED)** and associated harmonized standards.
- EnOcean is an **ISO/IEC 27001-certified company**, with certification applicable across all processes, procedures, and offerings, without exclusion from scope. Under this framework, EnOcean has already implemented a broad range of organisational, people, physical, and technical security measures. These include capabilities and practices aligned with core CRA expectations, such as **risk assessment, vulnerability management, access control, authentication, secure storage, secure communications, and continuity-related measures**.

This strong foundation positions us well to integrate CRA requirements efficiently and effectively.

Implementation Plan and Timeline

We are aligning our compliance program with the CRA's phased timeline:

Date	Milestone
10 December 2024	CRA enters into force (entry into legal effect)
11 June 2026	Applicability of rules for notification of conformity assessment bodies

11 September 2026	Start of reporting obligations for actively exploited vulnerabilities and severe incidents
11 December 2027	Full applicability: All products placed on the EU market must comply with CRA requirements

In compliance with the first obligations becoming applicable in **September 2026,** EnOcean has established and is maintaining processes for:

- receiving and assessing product-security vulnerability reports;
- communicating with reporters and, where appropriate, affected users;
- handling product vulnerabilities through a risk-based process;
- reporting actively exploited vulnerabilities and severe product-security incidents to the competent authorities where required; and
- maintaining supporting vulnerability management, incident-management and documentation processes.

Please see our Vulnerability Reporting and Coordinated Vulnerability Disclosure Policy.

For the broader cybersecurity requirements applicable from December 2027, EnOcean is currently establishing the **risk context** for each relevant product. This includes documenting the **intended purpose and reasonably foreseeable use** of the product, a **high-level description of the product architecture**, and the **assets forming the product**.

In parallel, we are preparing **Software Bills of Materials (SBOMs)** for relevant software deliverables in a machine-readable standard format. These SBOMs are intended to improve transparency regarding software components and dependencies and to support our vulnerability handling processes. Our SBOMs are generated in CycloneDX 1.6 JSON format and identify the relevant EnOcean product and firmware or software version, creation timestamp and known direct dependencies. You may find more details on this matter on our cybersecurity webpage: Cybersecurity at EnOcean

This work forms the basis for our **cybersecurity risk assessments** and supports a structured and consistent evaluation of relevant **threats, risks, vulnerabilities, and mitigation measures** across the product lifecycle. Our current approach is guided not only by the CRA legal requirements themselves, but also by the **BSI TR-03183 guidance series** published by the German authorities, which provides practical implementation guidance on topics such as risk assessment, SBOMs, and vulnerability handling. While the official harmonized European standards have not yet been fully adopted and cited at the time of this update, these guidances provide an important official basis for our current activities and allow us to move forward actively rather than waiting passively for the final standardization process to conclude. The outputs of these ongoing activities is being translated into a CRA-aligned framework for **user information, vulnerability management, and reporting governance**.

Following this phase, our work continues with the implementation and verification of the applicable **Annex I essential cybersecurity requirements**, as well as preparation for any required conformity assessment activities for relevant product categories. At the same time,

we are closely monitoring the ongoing European standardization work and aligning our programme with forthcoming harmonized standards as they become available, including standards covering:

- generic cybersecurity requirements
- vertical standards for important and critical product categories

Ongoing Engagement and Updates

The expected publication dates for the harmonized standards/guidelines may be subject to change. We understand our partners are seeking clarity in these times of regulatory evolution, and we are committed to providing transparency and updates as more guidance becomes available. As more technical details and guidance are published by the authorities, we will adapt our implementation accordingly.

We are confident that our established practices and early alignment efforts will ensure a seamless transition into CRA compliance, maintaining the high level of trust and reliability that our customers and partners expect from EnOcean.

If you have questions about how CRA may affect specific EnOcean products or require further information, please do not hesitate to reach out to compliance@enocean.com. To report a vulnerability of an EnOcean products, please contact cra@enocean.com.

July 30, 2026

EnOcean GmbH
Kolpingring 18a
82041 Oberhaching
Germany