STATEMENT OF LAUDA DR. R. WOBSER GMBH & CO. KG ON THE CYBER RESILIENCE ACT (CRA)

Lauda-Königshofen, 23 June 2026

The Cyber Resilience Act (CRA) is an EU regulation establishing mandatory cybersecurity requirements for products with digital elements. Its objective is to ensure the security of hardware and software products throughout their entire lifecycle – from development through market launch to the use phase.

LAUDA develops and manufactures products with digital elements that have a direct or indirect logical or physical data connection to a device or network (e.g. network-capable temperature control units and associated software). Certain product categories therefore fall within the scope of the CRA.

LAUDA is already systematically preparing the implementation of all CRA requirements at product and process level as part of an ongoing internal process. This encompasses both technical and organizational measures, ensuring that LAUDA reliably meets its manufacturers' obligations under the CRA by the prescribed deadlines.

IMPLEMENTATION OF CRA DEADLINES

The following overview shows the relevant phases:

PHASE 1 – REPORTING OBLIGATIONS

Products placed on the market before 11 September 2026 or placed on the market between 11 September 2026 and 10 December 2027.

From 11 September 2026, the reporting obligations pursuant to Article 14 CRA apply to all products with digital elements within the scope of the CRA. This also includes products that were made available on the EU market prior to full CRA application.

From 11 September 2026, LAUDA will report actively exploited vulnerabilities as well as serious security incidents to the competent authorities (CSIRT/ENISA):

- Early warning, without undue delay, in any case within 24 hours of becoming aware
- Notification with initial assessments, without undue delay, in any case within 72 hours
- Final report, within 14 days of a corrective measure becoming available (for actively exploited vulnerabilities); within one month of the notification (for serious security incidents)

In addition, affected users will be informed accordingly.

PHASE 2 – OTHER MANUFACTURER OBLIGATIONS

Products placed on the market from 11 December 2027 onwards:

From 11 December 2027, the full scope of CRA obligations applies. LAUDA will therefore additionally fulfil the following requirements, in particular for newly placed products falling under the CRA:

- Risk assessment and implementation of Security-by-Design and Security-by- Default (Art. 13 para. 1–4; Annex I Part I)
- Vulnerability management, including the creation of a Software Bill of Materials (SBOM); security updates will be provided after coordination (Art. 13 para. 8–11; Annex I Part II)
- Creation and maintenance of technical documentation (Art. 31; Annex VII)
- Issuance of the EU Declaration of Conformity and CE marking (Art. 28–30)
- Provision of complete user information, including a contact point and end of support period (Art. 13 para. 17, 19; Annex II)

CURRENT MEASURES AND OUTLOOK

LAUDA has already initiated the following concrete steps to implement the CRA requirements:

- PSIRT (Product Security Incident Response Team): LAUDA's PSIRT is currently being established and will serve as the central point of contact for product- related security incidents in the future.
- CVD Policy (Coordinated Vulnerability Disclosure): A strategy for coordinated vulnerability disclosure is being drawn up and is currently being implemented.
- Product Security Contact Point: The dedicated e-mail address psirt@lauda.de is already available today for security-related enquiries or customer reports. Incoming reports are forwarded internally to the departments responsible.
- The existing development process is currently being adapted regarding the CRA requirements. This includes, among other things, the further development of the existing cybersecurity risk assessment in accordance with the CRA requirements, a reassessment of products with digital elements on this basis, and, where necessary, targeted hardening based on the assessment results. In addition, the automated creation of the Software Bill of Materials (SBOM) as part of the building process is being introduced.

The relevant documents – including declarations of conformity and technical documentation – will be prepared as part of the ongoing process and made available in due course.

CONTACT

For enquiries regarding cybersecurity and CRA compliance, please contact:

LAUDA DR. R. WOBSER GMBH & CO. KG
Laudaplatz 1
97922 Lauda-Königshofen
Germany
E-Mail: psirt@lauda.de

Nina Kössel
Director Quality and Environmental Management