EU'S CYBER RESILIENCE ACT: THE CLOCK IS TICKING

In September 2026, new obligations under the Cyber Resilience Act ("**CRA**") will begin to take effect, with the regulation applying in full from 11 December 2027, following its entry into force on 10 December 2024. As a European Union ("**EU**") regulation with **extraterritorial effect**, it also imposes these obligations on Swiss manufacturers, software providers and distributors, requiring them to ensure compliance whenever their digital products are offered, supplied or distributed within the EU or European Economic Area ("**EEA**").

From **11 September 2026,** the **first binding obligation for manufacturers** takes effect, notably the **mandatory reporting of actively exploited vulnerabilities** (*i.e.*, digital product flaws already exploited by malicious actors in real-world attacks) **and severe security incidents.** Separately, affected Swiss companies will be required to systematically review and align their product security, development processes, supply-chain governance, and technical documentation in preparation for the CRA's product and lifecycle requirements becoming enforceable on 11 December 2027.

This briefing provides an overview of the CRA obligations coming into force in 2026 and 2027 and outlines the key steps Swiss companies need to take to meet these requirements.

SCOPE OF THE CRA

The CRA is the **first EU-wide cybersecurity regulation** for **all products with digital elements ("PDEs")** across all sectors. It establishes **uniform standards** and requires manufacturers and distributors to secure products throughout their **entire lifecycle.**

The CRA applies to **all PDEs placed on the EU/EEA market.** PDEs are defined as products capable of connecting to a network or another device, including:

- **Hardware products with connected functions**, such as smartphones, laptops, smartwatches, connected toys, microprocessors, firewalls, and smart meters;
- **Software products**, including accounting software, computer games, mobile apps; and
- **Remote data processing solutions integrated in PDEs**, e.g., cloud-enabled functionalities in smart home devices that allow users to remote-control the device.

Products already regulated under sector-specific EU legislation (e.g., medical devices, motor vehicles or certified aviation equipment) and purely non-commercial open-source software are excluded from the CRA's scope.

WHY SWISS COMPANIES SHOULD CARE

The **CRA applies to all companies involved in the manufacture, distribution, import or sale of PDEs in the EU/EEA**, irrespective of whether the company is established in the EU/EEA or not. **Swiss companies** fall under the CRA if they:

- Manufacture or develop PDEs in Switzerland and export them to the EU/EEA under their own brand (manufacturer role),
- Distribute PDEs into the EU/EEA (distributor role), or
- Modify existing PDEs before placing them on the EU/EEA market (in this case they may be treated as the manufacturer).

INCIDENT REPORTING BECOMES BINDING IN 2026

From **11 September 2026**, the CRA's **mandatory** incident reporting **obligation for manufacturers** for **actively exploited vulnerabilities** (for example, a zero-day vulnerability in a networked medical device or an industrial control system that is being actively exploited in the wild) and for **severe incidents affecting the security of PDEs** (for example, a ransomware attack or remote compromise that leads to loss of availability, integrity or confidentiality of a connected product deployed at scale) takes effect. Reporting must be filed with the **European Union Agency for Cybersecurity ("ENISA")**.

An **early-warning notification** must be submitted **without undue delay**, and in any event, **within 24 hours** of becoming aware of the incident, via the central EU platform operated by ENISA.

Where applicable, manufacturers must submit **follow-up reports within 72 hours**. **Final reports** must be submitted as follows:

- **Actively exploited vulnerabilities**: within 14 days of a corrective or mitigating measure becoming available; and
- **Severe incidents**: within one month of the initial 72-hour notification.

Manufacturers are also required to inform **users** of affected in-scope products **without undue delay**.

To handle such incidents and vulnerabilities, manufacturers must establish an internal **Computer Security Incident Response Team ("CSIRT")**.

The CRA's incident reporting requirements add complexity for manufacturers, as a single security incident may trigger multiple reporting obligations under different acts (e.g., the Swiss Federal Information Security Act, the Swiss Federal Data Protection Act, the GDPR), each with strict but differing deadlines.

FULL COMPLIANCE FROM 2027

From **11 December 2027**, the CRA introduces mandatory cybersecurity requirements, governing the planning, design, development, and maintenance of PDEs. The majority of these obligations fall on **manufacturers:**

- **Secure planning, design and development:** Manufacturers must integrate cybersecurity throughout the product lifecycle, *i.e.*, from the planning, design, and development to production, delivery and maintenance. Each PDE requires a documented cybersecurity risk analysis and must be developed with built-in cybersecurity features that minimize exploitable vulnerabilities and ensure data confidentiality and integrity. This follows the principles of "**secure by design**" and "**secure by default**", including controls such as authentication, access management, encryption, least-privilege principles, Denial-of-Service (DoS) resilience, secure boot mechanisms, and end-to-end security architecture.
- **Vulnerability management and lifecycle security:** Manufacturers must regularly update products to address emerging threats, handle identified vulnerabilities promptly, providing automatic security updates, and support products throughout a pre-defined "support period".
- **Conformity assessment**: Manufacturers must demonstrate compliance via the appropriate conformity assessment procedures, prepare a declaration of conformity and affix the CE marking on the product. For most **low-risk PDEs** (e.g., smart home devices, printers, or Bluetooth speakers), a **self-assessment** will be sufficient. **Higher-risk "important" PDEs** (e.g., firewalls, intrusion detection systems, operating systems and internet-connected toys) require a **third-party assessment** by authorised bodies or a **full quality assurance**. **High-risk "critical" PDEs** (e.g., hardware devices with security boxes, smart cards, smart meter gateways) are subject to stricter review. The European Commission designates PDEs as "important" and "critical" and may update the list over time.
- **Transparency and user information:** Manufacturers must provide technical documentation and clear, understandable instructions for safe use, including disclosing of known vulnerabilities or security considerations where relevant.

Distributors are also subject to specific obligations. In particular, before in-scope PDEs are placed on the EU market, they must verify that the product bears the CE marking, the required accompanying documentation is available, and the manufacturer has completed the required conformity assessment. Notably, they must also inform the manufacturer without undue delay upon becoming aware of any vulnerability.

CRA APPLIES TO EXISTING PRODUCTS

From **11 December 2027**, manufacturers may only place any product on the EU/EEA market if they **fully comply with the CRA**. This requirement applies to **every new unit**, including long-standing or unchanged products that have been sold for years, as the CRA assesses each individual product rather than product families. Any shipment, delivery, or first making available of a product to an EU distributor after this date must therefore meet all CRA obligations. In practice, that means that Swiss manufacturers must also ensure CRA compliance for products they have placed on the EU/EEA market **in unchanged form for years** if they want to continue placing these products on the EU/EEA market after 11 December 2027.

Only a **narrow sell-off exception** applies: products already lawfully placed on the EU market and **physically held in an EU distributor's inventory before 11 December 2027** may continue to be sold, even if they do not meet CRA requirements. This exception does not extend to subsequent deliveries, newly produced units, or products that are substantially modified after the deadline. A substantial modification includes changes such as software updates that alter the product's intended purpose or add new functionalities. Pure security or bug-fix updates generally do not trigger a new conformity assessment.

FINES

Violations of essential CRA requirements may result in **fines** of **up to EUR 15 million** or **2.5% of global annual (consolidated group) turnover**, whichever is higher, and authorities may additionally prohibit the placing of products on the market or order a recall.

PRACTICAL RECOMMENDATIONS FOR SWISS COMPANIES

Swiss companies should:

- **Make cybersecurity of connected products an executive priority**: Treat CRA implementation as a strategic, cross-functional program by assigning ownership and resources and requiring regular risk/compliance reporting.
- **Map their product portfolio and define role(s)**: Identify which products qualify as PDEs under the CRA definition. For each product, determine whether the company acts as a manufacturer or distributor when placing it on the EU/EEA market. If a Swiss company sells under its own brand or substantially modifies a product, such company may be considered a manufacturer. Swiss entities without an EU subsidiary or branch must appoint an EU-based importer or, where applicable, an authorized representative.
- **Prepare for reporting obligations:** Set up internal processes and responsibilities to meet CRA reporting obligations starting September 2026, including the ability to detect, document, and report actively exploited vulnerabilities and severe security incidents within the required timelines.
- **Classify products and select conformity routes**: Classify each PDE as non-critical or critical (class I/class II). Use internal control for non-critical products and involve an independent conformity assessment organization where required for critical classes. Prepare the EU declaration of conformity and affix the CE mark before placing on the market.
- **Conduct a CRA gap analysis**: Compare current product development, documentation, update, and maintenance processes with CRA requirements, and identify gaps (e.g., missing technical file, missing CE conformity process and marking, lack of end-user instructions).
- **Establish internal cybersecurity governance for PDEs**: Implement secure-by-design/default, define a support and maintenance policy (including a commitment to provide updates for each PDE over a pre-defined "support period"), and adopt a vulnerability management and coordinated disclosure process.
- **Build complete technical documentation**: Maintain a technical file evidencing conformity. Provide product specific user instructions and security guidance.
- **Traceability, supply-chain management and contracts:** Maintain comprehensive records of all suppliers and customers for at least ten years after placing each PDE on the market. Review and update supplier, distribution, and reseller contracts to allocate CRA-related responsibilities, require conformity evidence, and include audit and compliance clauses to ensure that suppliers comply with CRA obligations, particularly when they act as manufacturers or substantially modify products.
- **Plan post-market surveillance and corrective actions**: Monitor field performance, track vulnerabilities, and execute corrective measures (e.g., security updates, advisories, recalls) promptly. Keep evidence of conformity readily available for authorities.

AUTHORS

Dr. Christian Kunz
Partner
christian.kunz@baerkarrer.ch
T: +41 58 261 52 66

Dr. Katharina Cardon
Associate
katharina.cardondelichtbuer@baerkarrer.ch
T: +41 58 261 52 82

Ferdinand Rombach
Associate
ferdinand.rombach@baerkarrer.ch
T: +41 58 261 54 12