The EU's Cyber Resilience Act: What Swiss Businesses Need to Do Now

16.10.2026

Key takeaways

- **The Cyber Resilience Act (CRA) can apply to Swiss manufacturers supplying the EU market with products with digital elements.**
- **Specific reporting duties already apply, but the main product requirements follow on 11 December 2027.**
- **For Swiss businesses selling connected hardware or software in the EU, cybersecurity is becoming a condition of market access. The CRA introduces duties throughout the product lifecycle, and incident reporting is already mandatory.**
- **Switzerland is preparing its own cyber legislation. Businesses should already be responding to existing EU obligations.**

Which businesses and products are covered?

The CRA applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network ("Products with digital elements"). Examples include connected household appliances and mobile apps. Swiss manufacturers can be covered without an EU establishment; small and medium-sized enterprises have no blanket exemption. Sector-specific exclusions must be checked (Arts. 2–3 CRA).

Standalone cloud services generally fall outside the scope. However, cloud functionality developed under a manufacturer's responsibility and necessary for a product function can be included, such as centralized platform monitoring devices (e.g., centralized control of professional fridge temperature). Open-source software is not automatically exempt: the commercial context and the provider's role matter (for more details, see the Commission

guidance).

Reporting duties already apply

Since 11 September 2026, covered manufacturers must actively report exploited vulnerabilities and severe incidents affecting product security, including for products placed on the market earlier. Reports go through the EU Single Reporting Platform to the competent national incident response team and the EU cybersecurity agency, ENISA (Arts. 14, 16 and 69(3) CRA). This obligation applies as soon as a Swiss manufacturer sells Products with digital elements in the EU, even if it does not have an establishment within the EU.

An early warning is required without undue delay and within 24 hours of awareness; a more detailed notification must follow within 72 hours of awareness, also without undue delay. Final reports are due within 14 days after a corrective or mitigating measure becomes available for a vulnerability, or one month after the 72-hour notification for an incident (Commission reporting overview).

Prepare products and contracts for December 2027

From 11 December 2027, the main requirements will include secure design, a documented risk assessment, vulnerability handling, and security updates. Manufacturers must complete the applicable conformity assessment, issue an EU declaration of conformity, and affix the CE marking. Whether external assessment is needed depends on the product category and the assessment route available (more information can be found here for manufacturer obligations and conformity assessment).

Security support for products with digital elements must reflect their expected period of use: generally at least five years, potentially longer for long-lived products, or less if the expected lifespan is shorter. Supplier commitments and support budgets should be aligned accordingly (Art. 13(8) CRA).

What changes in Switzerland?

On 25 September 2026, the Federal Council commissioned a consultation draft for a standalone Swiss Cybersecurity Act to be prepared by June 2027. It is intended to address digital products, important digital data, and hosting and cloud providers. This is a distinct legislative project, not an enacted Swiss equivalent of the CRA (Federal Council announcement). However, the administration communicated that it intends to keep the administrative burden on businesses, especially for international corporations, to a minimum.

Do not forget other reporting duties

Existing Swiss reporting duties remain separate: certain personal data breaches trigger the duty to notify the Federal Data Protection and Information Commissioner under the Federal Act on Data Protection, while covered critical infrastructure operators must report qualifying cyberattacks under the Information Security Act to the National Cyber Security Centre. Notifying EU authorities does not automatically discharge these duties, even though the underlying information will, in many cases, be similar.

Next steps

- Identify covered products, EU sales channels and each entity’s legal role.
- Assign reporting responsibility and test escalation within the 24-hour deadline.
- Review supplier notification, security update, and support commitments; plan the required conformity assessment.
- Ensure alignment with various national and international reporting duties.

Authors: Michèle Burnier (Partner), Sarah Drukarch (Partner), Andrew Galantay (Junior Associate)

No legal or tax advice

This legal update provides a high-level overview and does not claim to be comprehensive. It does not constitute legal or tax advice. If you have any questions relating to this legal update or would like to have advice concerning your particular circumstances, please get in touch with your contact at Pestalozzi Attorneys at Law Ltd. or one of the contact persons mentioned in this legal update.

© 2026 Pestalozzi Attorneys at Law Ltd. All rights reserved.

***

Michèle Burnier

Partner
Attorney at law

Pestalozzi Attorneys at Law Ltd
Cours de Rive 13
1204 Geneva
Switzerland
T +41 22 999 96 00
michele.burnier@pestalozzilaw.com

Sarah Drukarch

Partner
Attorney at Law

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 93 23
sarah.drukarch@pestalozzilaw.com