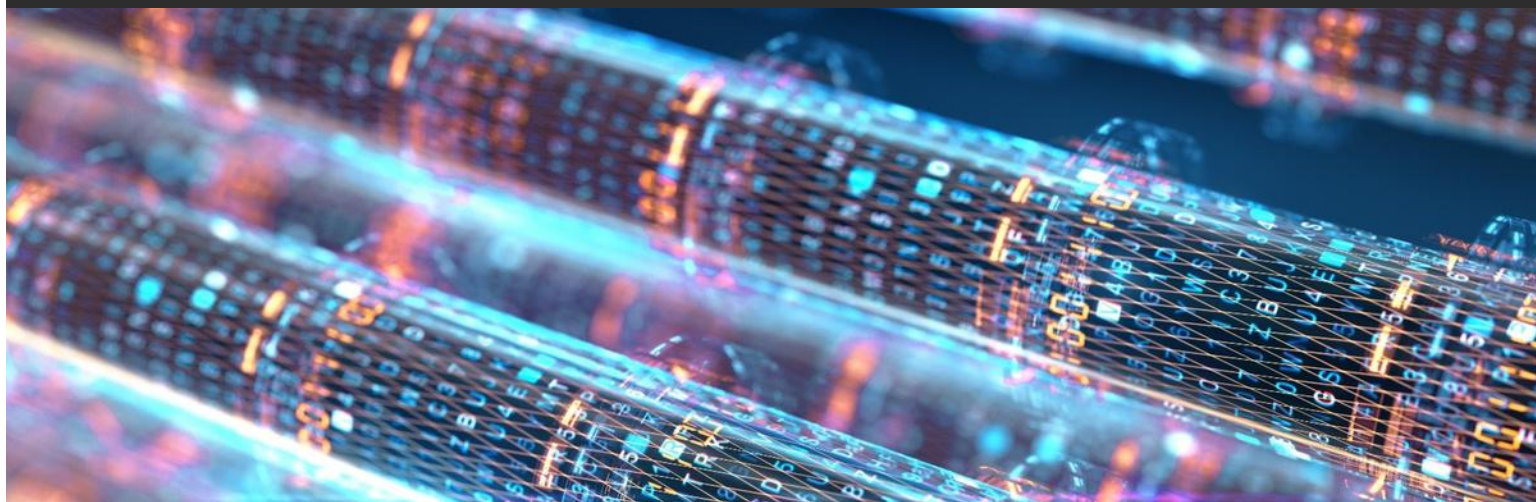


Alert | Data Privacy & Cybersecurity/Regulatory & Compliance



September 2026

EU Cyber Resilience Act (CRA) and Software: New Cybersecurity Obligations and CE Marking

[Read in German.](#)

The EU **Cyber Resilience Act** (CRA) makes cybersecurity a prerequisite for access to the EU market, not only for hardware products with digital elements, but also for software placed on the market independently. Its core requirements are far-reaching: conformity assessments, European Conformity (CE) marking, and a duty to supply security updates free of charge throughout a defined support period. For some providers, meeting them might mean rethinking established go-to-market processes and pricing models from the ground up.

This issue is particularly relevant right now: While software and other products with digital elements do not need to comply with these obligations until Dec. 11, 2027, the process required for a first CE conformity assessment may require significant lead time. The requirements also apply to products developed or manufactured before Dec. 11, 2027, if they are placed on the market after that date. In addition, reporting requirements for actively exploited vulnerabilities and severe security incidents have already taken effect.

What Software Falls Within the CRA's Scope?

The CRA applies to what it calls “products with digital elements.” These include:

- Software products made available independently on the market, such as on-premises software, including downloadable tools, apps, agents, SDKs, and client libraries;
- embedded software, firmware, and – possibly – connected systems;
- hardware products with digital elements (mostly: IoT products), including hardware or software components offered separately (such as the embedded software and firmware noted above);
- certain cloud solutions designed and developed by the manufacturer, or under its responsibility, that the product with digital elements needs in order to perform one of its functions and
- free and open-source software – although here the regulatory requirements differ from those applicable to ordinary software (see below).

This broad scope of application is intentional: The European Commission describes the CRA as a horizontal framework covering hardware and software products made available on the EU market.

SaaS, Cloud, and Installable Components: Where the CRA Applies

Pure SaaS and other cloud services generally fall outside the CRA, because they are typically offered on the market as a “service” rather than a “product.” The analysis changes, however, where a cloud or SaaS solution is necessary to deliver a function of a product with digital elements and was designed and developed by the manufacturer, or under its responsibility (a so-called remote data processing solution).

A practical example illustrates the point. A smart security camera records images and video locally, but its core functionality is the AI-supported detection of people, vehicles, or security-related events that runs through a cloud application operated by the manufacturer. Because those analysis and alert functions do not work without the cloud connection, the cloud application is a functional component of the product. It therefore falls under the CRA as a remote data processing solution, alongside the camera itself.

Who Is Subject to CRA Obligations?

The primary addressee is the manufacturer, i.e., the person or entity that develops or manufactures a product with digital elements, and markets it under its own name or trademark. Manufacturer obligations also apply to a person that makes substantial modifications to a regulated product and places the modified product on the market.

Importers and distributors are subject to separate verification, due diligence, and compliance obligations.

The CRA also establishes a distinct regime for “open-source software stewards,” including requirements to establish and document a cybersecurity strategy, cooperate with market surveillance authorities, and comply with specified reporting obligations.

Internally, the CRA reaches several functions at once:

- Product, Engineering, and DevSecOps must operationalize “secure-by-design” requirements and integrate them into the development process.
- Legal and Compliance must assess manufacturer status, risk category, and the conformity process.

- Management and go-to-market teams must ensure that the applicable (usually, CE) conformity assessment has been completed, the required technical documentation and EU declaration of conformity are in place, and CE marking has been affixed before the product is placed on the EU market.

What Specific Measures Must Responsible Parties Implement Under the CRA?

Secure by design

Risk assessments, secure default settings and access controls, a traceable security architecture, and structured vulnerability handling must be built in from the design and development stages and maintained across the entire product lifecycle.

Once relevant harmonized European standards are available, manufacturers may use them to benefit from a presumption of conformity with the relevant CRA requirements. Until then, existing European and international cybersecurity standards may provide useful technical guidance, but do not in themselves create a presumption of conformity with the CRA.

Free security updates will be mandatory

Manufacturers must remediate vulnerabilities free of charge through security updates during the support period, and must keep those updates available for at least 10 years after release or for the remainder of the support period, whichever is longer. This support period is mainly determined by reference to the product's expected period of use, and generally is at least five years.

Reporting

Already since Sept. 11, 2026, manufacturers must report actively exploited vulnerabilities and severe incidents through the European Union Agency for Cybersecurity (ENISA)'s CRA Single Reporting Platform. An early warning is due within 24 hours of becoming aware of the vulnerability or incident, followed by a vulnerability or incident notification within 72 hours. For actively exploited vulnerabilities, the final report is due no later than 14 days after a corrective or mitigating measure becomes available; for severe incidents, it is due within one month after submitting the 72-hour incident notification.

Technical Documentation, Software Bill of Materials (SBOM), and Documentation Requirements

Missing or inadequate technical documentation poses significant risks. Manufacturers must prepare and maintain the documentation the CRA requires, including the product's cybersecurity risk assessment and technical documentation supporting the applicable conformity assessment. The CRA also requires manufacturers to identify and document vulnerabilities and product components, including by drawing up a SBOM in a commonly used and machine-readable format covering at least the product's top-level dependencies. Companies may also wish to maintain robust processes for vulnerability reporting, security updates, and regulatory inquiries.

Exception for Tailor-Made Software and Test Versions

The CRA allows for (limited) flexibility for tailor-made products. Where a product is developed for a specific business user for its particular purpose, and manufacturer and user expressly agree different contractual terms, they may deviate from two specific requirements: the requirements for a secure-by-default configuration, and for free security updates. Limited exceptions also apply to "unfinished

software” made available for testing purposes, and to products presented at trade fairs, exhibitions, and similar events. In each case, the CRA imposes specific conditions, including appropriate indications that the product does not yet comply with the CRA and restrictions on making it available until compliance has been achieved.

Special Provisions for SMEs

For microenterprises and small and medium-sized enterprises (SMEs), the CRA offers a range of targeted support: Member State initiatives on training, awareness, information, and testing opportunities; third-party assessments; and regulatory sandboxes. Microenterprises and small enterprises may also prepare technical documentation using a simplified form, which the European Commission will prepare. Further support is available through the Digital Europe Program, which offers relevant funding and support projects for affected companies.

Conclusion

For software companies, the CRA is not just an IT security matter. It reshapes how products are developed, documented, priced, and marketed, and compliance may significantly delay sales in the EU market, while non-compliance might prevent it. At the same time, the CRA establishes a harmonized legal framework that may strengthen trust in security-sensitive markets.

Authors

This GT Alert was prepared by:

- **Viola Bensinger** | +49 30.700.171.150 | Viola.Bensinger@gtlaw.com
- **Jana Rudt** | +49 30.700.171.336 | Jana.Rudt@gtlaw.com

Abu Dhabi[†]. Albany. Amsterdam. Aspen. Atlanta. Austin. Berlin[~]. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Dubai[†]. Fort Lauderdale. Houston. Las Vegas. London^{*}. Long Island. Los Angeles. Mexico City⁺. Miami. Milan^{*}. Minneapolis. Munich[~]. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Riyadh^{*}. Sacramento. Salt Lake City. San Diego. San Francisco. São Paulo[»]. Seoul[»]. Shanghai. Silicon Valley. Singapore[»]. Tallahassee. Tampa. Tel Aviv[^]. Tokyo[»]. Warsaw[~]. Washington, D.C. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. Greenberg Traurig's Abu Dhabi office is a branch of Greenberg Traurig, P.A., which is registered with the Abu Dhabi Global Market Registration Authority (Registration No. 29906) and licensed to carry out legal services and regulated as a DNFBP by the ADGM Financial Services Regulatory Authority. ~Greenberg Traurig's Berlin and Munich offices are operated by Greenberg Traurig Germany, LLP, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. <Greenberg Traurig's Dubai office is operated by Greenberg Traurig Limited, a company registered in the Dubai International Financial Centre (Registration No. CL7238), regulated as a DNFBP by the Dubai Financial Services Authority and licensed by The Government of Dubai Legal Affairs Department. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Studio Legal Associato, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. «Greenberg Traurig operates in the Kingdom of Saudi Arabia through Greenberg Traurig Khalid Al-Thebity Law Firm, a professional limited liability company, licensed to practice law by the Ministry of Justice. »Greenberg Traurig's São Paulo office is operated by Greenberg Traurig Brazil Consultores em Direito Estrangeiro – Direito Estadunidense, incorporated in Brazil as a foreign legal consulting firm. Attorneys in the São Paulo office do not practice Brazilian law. »Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ~Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. »Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAURIG Nowakowska-*

Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2026 Greenberg Traurig, LLP. All rights reserved.