Cybersecurity Law Report cslawreport.com

Jan. 28, 2026

Mobile Technology

What International Companies Should Do to Comply With the E.U. Cyber Resilience Act

By Rita Heimes and Jenny Arlington, *Akin*

The European Union has chosen a proactive approach to cybersecurity regulation, and the comprehensive, industry-agnostic E.U. cyber law with extraterritorial impact – the Cyber Resilience Act (CRA) [1] – represents one of the most significant cybersecurity regulations affecting digital products to date, globally.

Imposing secure-by-design requirements before products enter the E.U. market, and ongoing security obligations for at least five years thereafter, the CRA's scope is broad, capturing virtually any software or hardware that connects to a network. Additionally, its penalties are steep, including fines up to €15 million (approximately $17.5 million) or 2.5 percent of global turnover, whichever is higher, and an obligation on manufacturers to correct immediately any noncompliance, or withdraw or recall the product. Regulatory authorities have the power to restrict or prohibit noncompliant products from entering the E.U. market, or to ensure that they are recalled or withdrawn. "Important" and "critical" products face even stricter and more burdensome obligations.

With obligations phasing in from June 2026 to December 2027, and mandatory vulnerability reporting beginning September 11, 2026, companies must begin preparations now. This article outlines the CRA's core requirements and offers five priority steps international businesses should take to remain compliant and operational in the E.U.

See this two-part series on cybersecurity obligations in the E.U.'s Digital Laws: "AI Act, CRA and NIS2" (Sep. 4, 2024), and "Data Act, DORA and Compliance Steps" (Sep. 11, 2024).

Understanding the CRA's Extensive Reach

The CRA is much broader and stricter than most other worldwide cybersecurity laws.

Products With Digital Elements

A wide range of products are caught under the law, as it applies to "products with digital elements" – an expansive term covering both hardware and software products, including hardware and software

components, along with their remote data processing solutions. This includes everything from smart meters, home virtual assistants and household appliances, through smartphones, mobile applications and computer games, as well as routers, operating systems, browsers, firewalls, intrusion detection and prevention systems, security information and event management (SIEM) systems, personal wearable products, smartcards (including payment and access cards) and industrial control or infrastructure software, machinery and robots. There are certain limited exemptions for open-source software that is not monetized.

AI tools and systems are also caught under the CRA – as well as under the E.U. Artificial Intelligence Act (E.U. AI Act), which is discussed further below. Overall, if a product connects to a device or network, either directly or indirectly, it likely falls within the CRA's scope. In addition, the CRA places more burdensome obligations in relation to "important" and "critical" products, as discussed further below.

Economic Operators Across Sectors

International economic operators across all industry sectors will be regulated by the CRA if they:

- manufacture or develop products with digital elements or have products with digital elements designed, developed or manufactured, and they market such products under their name or trademark in the E.U., whether for payment, monetization or free of charge;
- are the authorized representatives of such manufacturers or developers in the E.U.;
- import such products into the E.U.;
- distribute such products in the E.U.; or
- carry out a substantial modification of a product with digital elements and make that product available on the E.U. market.

Key Obligations for Manufacturers

Manufacturers that market products with digital elements in the E.U. under their own name or trademark are subject to broad and strict obligations under the CRA, including:

- ensuring that the products have been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Annex I of the CRA;
- putting in place procedures for handling vulnerabilities effectively and in accordance with the essential cybersecurity requirements;
- determining a support period of a minimum of five years (unless the lifespan of the product is shorter) during which the manufacturer is required to ensure that vulnerabilities are handled effectively and in accordance with the essential cybersecurity requirements;
- drawing up technical documentation, as well as information and instructions for the user, before placing the product on the E.U. market;

- arranging the applicable conformity assessment procedures, drawing up the relevant declaration of conformity and arranging the proper affixation of the "CE marking" that signifies conformity with the CRA;
- in case the product is not in compliance with the essential cybersecurity requirements, immediately taking corrective measures to bring the product into compliance, or withdraw or recall the product; and
- reporting actively exploited vulnerabilities initially within 24 hours of becoming aware of them, with further reports submitted within 72 hours and following corrective or mitigating measures.

See "In New Proposal, E.U. Aims to Boost Security of Connected Devices" (Nov. 2, 2022).

Requirements for Importers and Distributors As Well

Relying on importers or distributors for the marketing of products in the E.U. does not negate the need for compliance with the CRA. Importers and distributors also have strict obligations, which they will likely flow down to the manufacturers to ensure their own compliance with the CRA. For example, importers and distributors must ensure that products with digital elements have undergone the appropriate conformity assessments, have the necessary technical documentation and information and instructions for the user, and bear the "CE marking" prior to being placed on the E.U. market.

Compliance Deadlines

At the end of summer 2026, businesses must be in position to report any actively exploited vulnerability to the relevant regulators – which necessarily entails having taken steps to consider how the CRA applies to their products and operations.

At the end of 2027, businesses must be in full compliance. It is essential that affected companies take steps now to allow products in research and development to be market-ready when the CRA comes into full force.

Five Top Priority Implementation Actions Businesses Should Consider

The CRA represents a fundamental shift in how digital products are regulated, placing cybersecurity on par with other essential safety and quality requirements. For international companies serving the European market, compliance will be a prerequisite for market access. Companies that prepare now, implementing the recommendations below, have time to build necessary capabilities, adjust products and processes, and establish compliance infrastructure.

Determine Which Products and Components Are Covered by the CRA

Companies must identify which products fall under the CRA's scope by carrying out a detailed analysis of each product's digital elements, connectivity features and market presence in the E.U.

For best results, companies should create a cross-functional team including product management, engineering, marketing/distribution/sales, legal and compliance to review the entire digital product portfolio. A well-run project will result in an inventory of each product's purpose, data processing capabilities, connectivity features, and any third-party components or open-source software it incorporates.

All products with digital elements must comply with, among other things, the essential cybersecurity requirements – and manufacturers must demonstrate conformity by, at the very least, undertaking an internal control procedure, drawing up an E.U. declaration of conformity available to the regulators on request and affixing the "CE marking" to their products.

Products that might be categorized as "important" or "critical" require particular attention, as they are subject to more burdensome requirements. Products are classified depending on their cybersecurity-related functionalities and the level of cybersecurity risk they might pose. The Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 shed light on the "important" and "critical" product categories, clarifying that products with core digital functionalities (such as operating systems or password managers in smartphones) fall under these stricter rules, ensuring enhanced cybersecurity for essential goods, and detailed how integrated digital elements affect a product's classification. Additionally, the European Commission can amend and supplement the categories of important and critical products via delegated acts, which can be adopted more quickly than legislation.

Important Products

Article 7 and Annex III of the CRA include the categories of "important" products, split into two classes. Class I important products include identity management systems (such as single sign-on software, multi-factor authentication software and hardware authentication devices), browsers, password managers, virtual private networks, software that detects or searches for malicious software, SIEM systems, operating systems, routers, smart home virtual assistants, smart home devices with security features (such as alarm systems) and personal wearable products (such as fitness trackers and smartwatches). Class II important products – subject to even stricter requirements – include firewalls, intrusion detection and prevention systems, and tamper-resistant microprocessors.

Manufacturers of products falling into the listed categories of important products must apply, where these exist, harmonized standards, common specifications or a European cybersecurity certification scheme achieving at least a "substantial" assurance level. The three European standardization organizations (CEN, CENELEC and ETSI) are working on uniform harmonized European standards to support the implementation of the CRA for certain product categories and are aiming to finalize all necessary standards by December 2026. Where standards, common specifications or cybersecurity schemes are not applicable, important products will have to undergo a third-party conformity assessment (as set forth in Article 32(2) and (3) and Annex VIII of the CRA).

Critical Products

Article 8 and Annex IV of the CRA list the "critical" product categories, which include hardware devices with security boxes (such as physical payment terminals), smart meter gateways, and smartcards or similar devices (such as access cards and payment cards). Critical products must comply with a European cybersecurity certification scheme, where this exists, achieving at least a "substantial" assurance level, or undergo a third-party conformity assessment.

Prepare to Manage Post-Sale Product Vulnerabilities and Support

Managing Vulnerabilities

Businesses should consider setting up processes now to be able to identify and document vulnerabilities, assess their severity and exploitability, develop and test patches, and deploy updates to users – all within tight time frames.

Globally, product liability frameworks usually focus on defects at the time of sale. The CRA, however, imposes obligations not only pre-market, but also throughout a product's "support period" (discussed below). If vulnerabilities are discovered post-sale, the CRA requires manufacturers to assess, document and remediate without delay, as well as to publicly disclose information about fixed vulnerabilities. Importers and distributors have an obligation to inform the manufacturers upon becoming aware of a vulnerability, and inform the regulatory authority upon becoming aware that a product poses a significant cybersecurity risk.

If a vulnerability is "actively exploited" by a malicious actor, manufacturers have 24 hours to report it to a designated Computer Security Incident Response Team and the E.U. agency dedicated to cybersecurity (ENISA). This early warning notification must be followed by a more detailed vulnerability notification within 72 hours and a final report within 14 days of a corrective measure becoming available. Missing these deadlines – and/or other noncompliance with the CRA – can result in substantial fines.

Equally important is the obligation to establish a coordinated vulnerability disclosure policy. The CRA mandates that manufacturers create clear processes for security researchers and other third parties to report vulnerabilities. This policy should specify how reports will be received, acknowledged, assessed and acted upon, while protecting the confidentiality of reporters who act in good faith and allowing manufacturers to remedy vulnerabilities before detailed information is disclosed publicly.

For manufacturers of consumer digital products planning to mitigate discovered vulnerabilities through automated product updates, the CRA requires that users retain the ability to opt out through a clear mechanism – an obligation that manufacturers should consider in the design phase as well.

Providing Support

As a feature of vulnerability mitigation, the CRA imposes a mandatory post-sale support period during which manufacturers must handle vulnerabilities and provide security updates. The default is five years unless the product's lifetime is genuinely shorter (or longer).

Manufacturers are obligated to determine and document the relevant support period by taking into account reasonable user expectations, the nature and intended purpose of the product, relevant E.U. law determining product lifetimes, typical use periods for similar products, and the availability of operating environments and third-party components.

Businesses should consider what the support period should be in light of their operations and commercial model.

The support period must be clearly communicated to users at the time of purchase and displayed on the product. Market surveillance authorities are tasked with monitoring how support periods are determined, and a newly established dedicated administrative cooperation group (ADCO) – which consists of representatives of the market surveillance authorities and aims to support the uniform application of the CRA across the E.U. – will publish statistics on support periods by product category.

Implement Secure-by-Design Principles Across Development

The CRA requires products to be "designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks." This means embedding security throughout the product development lifecycle while maintaining documentation of all relevant steps.

Businesses should consider having an enterprise-level policy for developing products with security by design, and integrating this policy into risk assessments, audits and board reporting. Appropriate standards can calve off that policy, leading to guidelines and ultimately step-by-step documentation integrated into product design, development and quality assurance processes.

The documented risk assessments should address potential threats, vulnerabilities and impacts via design choices that minimize attack surfaces and implement appropriate security controls. The CRA requires products to be made available on the market "without known exploitable vulnerabilities" – a high bar that demands rigorous pre-release security validation.

See "Lessons From SolarWinds" (Jan. 26, 2022).

Vet Supply Chain by Creating Comprehensive Software Bills of Materials

The CRA holds manufacturers responsible for the security of their complete products, including integrated components. Thus, manufacturers must identify and document all product components and – for software – general software bills of materials (SBOMs), which must be in a "commonly used and machine-readable format" and cover "at the very least the top-level dependencies of the products." The reports can be automated, but implementing SBOM generation requires understanding the entire software supply chain, including third-party libraries, open-source components and dependencies.

Building even more robust security vetting into the supply chain is paramount for compliance. Not only must due diligence validate that components are secure-by-design and documented accordingly, but, if vulnerabilities are later detected in supplied components, the purchasing business must inform the component manufacturer and address the vulnerability in its own down-stream product.

The CRA's requirements must be addressed in supplier agreements. Although component producers may seek to prevent certain testing on intellectual property rights grounds, businesses should push back on that, stressing the manufacturer's legal compliance duties under the CRA.

See "Using Software Bills of Materials to Bolster Security in Contracting" (Sep. 28, 2022).

Initiate Outside Counsel and Regulator Relationships

Demonstrating compliance with the CRA is vital; businesses must develop and implement policies concerning cybersecurity and vulnerability management and document risk assessments. In light of the broad powers of regulatory authorities to request such documentation, businesses should consider confirming the appropriate level of disclosure with trusted outside counsel. In case of communications with market surveillance authorities – in the event of noncompliance, exploited vulnerability, severe incidents or significant cybersecurity risks – businesses would be well-advised to engage outside counsel to navigate more complex questions or risk of investigations.

With assistance from counsel, businesses should determine which E.U. Member State will serve as the organization's primary point of contact, including in cases of reporting vulnerabilities. For manufacturers with establishments in the E.U., that will be the Member State where the "main" establishment is located. For international companies without E.U. establishments, complex rules determine the appropriate Member State based on authorized representatives, importers, distributors or user locations. For some manufacturers, having an authorized local representative can be beneficial for managing documentation, communicating with market surveillance authorities and serving as a local compliance interface. Counsel can assist with this analysis and making the appropriate local connections.

Now is the time to build relationships with the relevant market surveillance authorities across the E.U. – before investigations and enforcement actions arise. These authorities will monitor CRA compliance and have broad investigatory powers. They can request technical documentation, conduct product testing, require access to data for assessment purposes, act in situations where they have sufficient reason to consider that a product presents a significant cybersecurity risk, and impose substantial fines for noncompliance as well as any other corrective or restrictive measures. Some authorities may offer guidance or pre-market consultations, particularly for novel products or complex compliance questions. Understanding their priorities and approaches can help organizations address potential concerns proactively.

Additional Strategic Considerations for Compliance Across the E.U.'s Digital Regulatory Landscape

The CRA is part of the E.U.'s broad digital strategy, launched in 2019, which aims to encourage innovation in digital technology while minimizing any negative risks. The CRA complements the NIS2 Directive on cybersecurity of network and information systems and the GDPR – and under the E.U.'s Digital Omnibus proposal, these laws will be further connected through the establishment of a single-entry point of vulnerability, incident and breach reporting.

Additionally, the CRA interacts with various sector-specific regulations by excluding, for example, medical devices and vehicle and civil aviation components from its scope, as they are subject to separate E.U. laws. The CRA also works together with the E.U. AI Act. AI systems classified as high-risk AI systems under the E.U. AI Act are subject to cybersecurity requirements thereunder. If such systems comply with the essential cybersecurity requirements of the CRA and manufacturers have put in place vulnerability handling requirements in accordance with the CRA, the AI tools and systems will be deemed to comply with the applicable cybersecurity obligations under the E.U. AI Act, as well.

An appropriate goal for businesses in 2026 is to develop an integrated compliance strategy that addresses these overlapping requirements efficiently. In many cases, security measures implemented for CRA compliance will support GDPR data protection objectives or NIS2 supply chain security requirements. Conversely, privacy-by-design approaches required under the GDPR complement the CRA's secure-by-design mandate.

Businesses should stay tuned for harmonization standards providing technical specifications for CRA compliance or, alternatively, common specifications covering technical requirements where harmonized standards are unavailable or inadequate. Products conforming to these standards or specifications benefit from a presumption of conformity with the essential cybersecurity requirements mandated by the CRA.

See this three-part series answering top questions about the E.U. AI Act: "Reach and Unique Requirements" (Apr. 24, 2024), "Risk Tiers and Big-Player Transparency" (May 1, 2024), and "Practical Steps and What's Next" (May 8, 2024).

The Cost of Inaction

The financial implications of CRA noncompliance can be severe, with the potential for administrative fines to reach €15 million or 2.5 percent of global annual turnover, and lower but still substantial penalties for documentation and procedural violations. Beyond direct fines, noncompliant products can be withdrawn from the market, recalled or prohibited from sale in the first instance, which could deal a significant blow to firm revenue and damage brand reputation. Where products are in breach of the CRA, there is also a risk of representative actions, *i.e.*, class actions, which have been on the rise in the E.U.

Perhaps more significantly, the CRA creates a competitive dynamic where compliance becomes a market differentiator. As the CRA is further publicized among consumers and businesses, they may prefer products bearing the CE marking and demonstrating CRA compliance. Companies that achieve early compliance can leverage this as a competitive advantage.

Rita Heimes is a senior counsel in Akin's Washington, D.C. office, where she supports clients across industries with incident response, cybersecurity preparedness and regulatory compliance, and privacy and data protection issues, globally. Prior to joining Akin, Heimes was GC and CPO for the world's largest privacy organization – the IAPP. She brings more than 20 years of experience in complex, data-related transactions and disputes.

Jenny Arlington is a senior counsel in Akin's London office, where she assists global companies across multiple industry sectors, including technology, energy, funds, multinational conglomerates and enterprises handling big data, with compliance and in investigations involving data protection, privacy and cybersecurity issues. She also advises clients on developing and deploying machine learning and AI tools and systems, and handles complex international disputes, both arbitrations and litigations.

[1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).