

The EU Cyber Resilience Act

Herzog's Guide





INTRODUCTION

Recently, the **reporting obligations** under the EU [Cyber Resilience Act](#) (Regulation (EU) 2024/2847) ("**CRA**") have **entered into force**.

The CRA establishes a new, horizontal cybersecurity framework for hardware and software products made available on the EU market. It is particularly relevant to companies that develop, manufacture, distribute or import **products with digital elements**, including software, connected devices, hardware products and products incorporating digital functionality. The CRA applies where the product's intended purpose or reasonably foreseeable use includes a direct or indirect, logical or physical data connection to a device or network. Given the CRA's broad definition of a "product with digital elements", this will generally include **mobile applications and other software products** that connect to a device or network.

The CRA makes cybersecurity an integral part of product compliance, with requirements applying to the **design, development and production** of products and to vulnerability handling throughout the relevant support period.

The CRA's main requirements will apply from **11 December 2027**. However, its mandatory reporting regime is already applicable as of **11 September 2026**.

In addition, on 27 July 2026, the European Commission published [practical guidance](#) ("**Guidance**") to assist companies in understanding the CRA's requirements and preparing for its implementation, including in relation to scope, support periods, substantial modification, risk assessment and reporting.

Below is an overview of the key provisions and practical implications of the CRA.



**1****Scope and Application - Which Products Are Covered?**

The CRA applies to "products with digital elements" that are made available on the EU market. The definition covers software and hardware products and their remote data-processing solutions, including software and hardware components placed on the market separately.

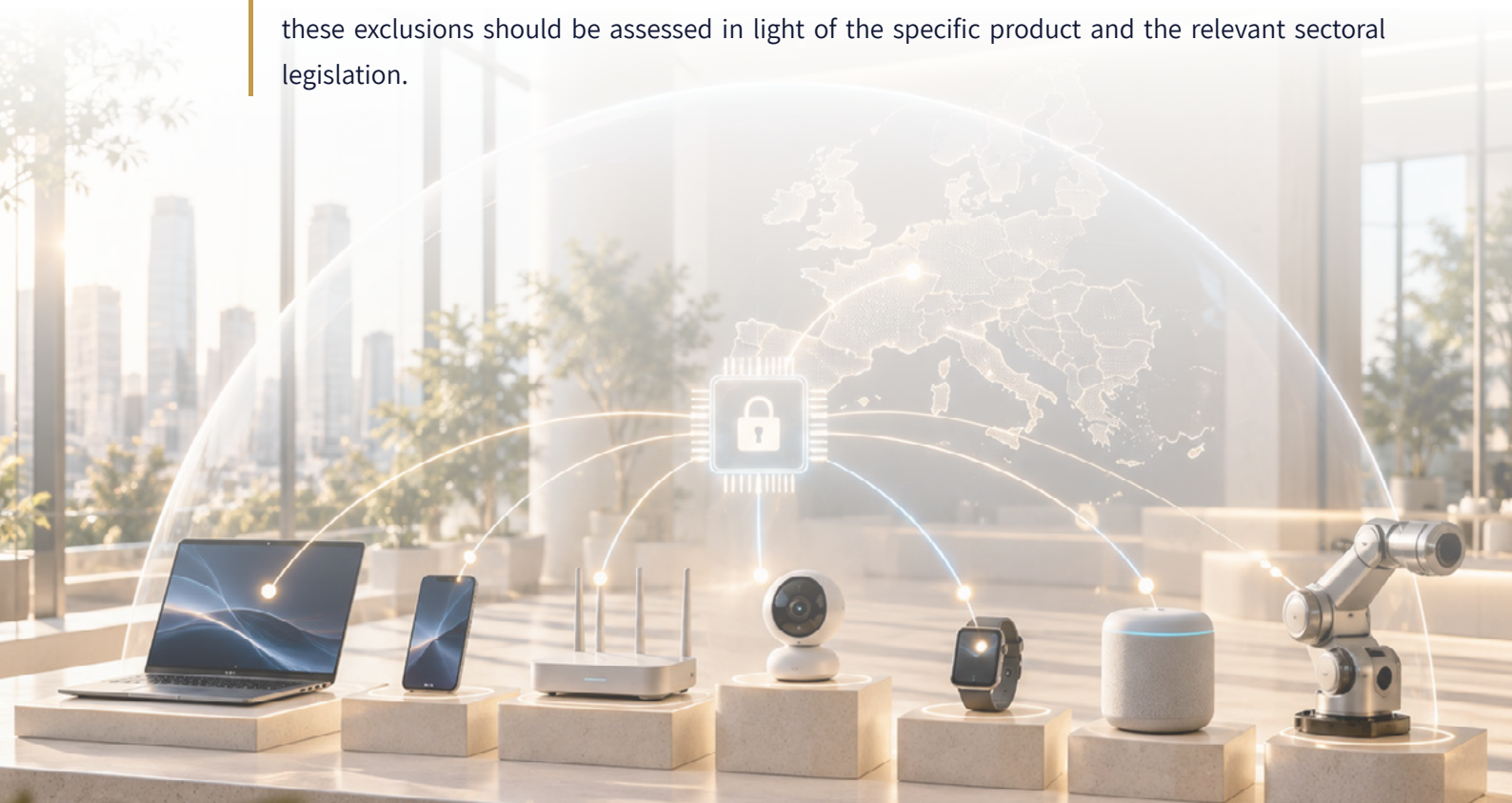
The concept therefore extends beyond traditional connected devices and may cover a broad range of products, including **software applications**, operating systems, connected hardware, network products and other products incorporating software or firmware.

The CRA also covers certain remote data-processing solutions where the software for the processing is designed and developed by or for the manufacturer and the absence of that processing would prevent the product from performing one of its functions. This can be relevant to **products relying on cloud-based functionality** or other remotely provided functionality that is integral to the operation of the product. The EC's July 2026 Guidance provides further clarification and practical examples concerning this distinction. Accordingly, whether a remote data-processing solution falls within the CRA should be assessed on a product-by-product basis, by reference to the specific statutory definition and whether the processing is necessary for the product to perform one of its functions.



The CRA is generally triggered by a **product being made available on the EU market**, rather than by the location of the manufacturer. Accordingly, companies established outside the EU may also be subject to the CRA where their products are made available in the EU.

The CRA also provides for specific exclusions and limitations, including for certain products already subject to other EU legislation, products developed or modified exclusively for national security or defense purposes, and certain free and open-source software. The applicability of these exclusions should be assessed in light of the specific product and the relevant sectoral legislation.



**2****Who Has Obligations Under the CRA?**

The CRA allocates obligations among different economic operators, including manufacturers, authorized representatives, importers and distributors.

A company will generally be regarded as a manufacturer where it manufactures a product, has a product designed or manufactured, and markets that product under its own name or trademark. A person that substantially modifies a product after it has been placed on the market may also become subject to manufacturers' obligations in accordance with the CRA.

Importers and distributors have separate obligations, including ensuring that relevant conformity, documentation, identification and information requirements have been met before making products available on the EU market. An authorized representative may also have specific obligations under the CRA, where appointed by a manufacturer.



Companies operating through multiple group entities should therefore identify, for each in-scope product, which entity is acting as the relevant economic operator and where responsibility for the CRA requirements sits.

3**What Are the Main CRA Requirements?**

The CRA establishes a lifecycle-based cybersecurity framework for manufacturers. Among other things, manufacturers will be required to:



Security by design, default and risk management - design, develop and produce products with digital elements in a manner that addresses cybersecurity risks throughout the relevant lifecycle and, where applicable, ensure that products are securely configured by default, based on a documented cybersecurity risk assessment that takes into account the product's intended purpose, reasonably foreseeable use and operating environment;



Vulnerability management and security updates - establish processes for identifying, assessing and addressing vulnerabilities, including coordinated vulnerability disclosure, security testing and reviews, and mechanisms for securely distributing security updates;



Third-party components and software transparency - exercise due diligence when integrating third-party components, including FOSS (Free and Open-Source Software), and maintain an SBOM (Software Bill of Materials) in a commonly used and machine-readable format covering, at a minimum, the product's top-level dependencies;



Technical documentation, user information and support - prepare and maintain technical documentation demonstrating compliance, including the cybersecurity risk assessment, and provide users with information and instructions on secure installation, operation, updates, support and decommissioning, as well as determine and effectively maintain an appropriate support period; and



Conformity assessment and CE marking - before placing a product on the EU market, complete the applicable conformity-assessment procedure and draw up the EU Declaration of Conformity and affix the CE marking where required.

4 Important and Critical Products - Additional Requirements

The CRA establishes a tiered **conformity-assessment framework** for products that are particularly relevant from a cybersecurity perspective. It distinguishes between “important products with digital elements”, divided into Class I and Class II under Annex III, and “critical products with digital elements” under Annex IV.

A product falls within these categories where it has the core functionality of a product category specified in the relevant Annex:



Important products (Class I) include, among others, certain operating systems, browsers, password managers, VPNs, network-management and security products, and internet-connected network equipment;



Important products (Class II) covers, among others, certain hypervisors, container runtimes, firewalls and intrusion detection and prevention systems.



Critical products comprise a narrower set of categories, including certain hardware security devices, smart-meter gateways and smartcards or similar devices with secure elements.

The classification is significant because it determines the conformity-assessment procedure that must be followed. **Class I** products may, subject to the conditions set out in the CRA, rely on **internal control**, while **Class II** and **critical products** are generally subject to more stringent conformity-assessment procedures, including **third-party assessment** or, where available and applicable, a relevant European cybersecurity certification scheme.



Companies should therefore map their product portfolios against Annexes III and IV at an early stage, as the classification may materially affect the applicable conformity-assessment procedure and the compliance work required before the product is placed on the EU market.



5

Reporting Obligations

As mentioned, the CRA's reporting obligations have **entered into force** on **11 September 2026**. Manufacturers are required to report:

- Actively exploited vulnerabilities contained in products with digital elements; and
- Severe incidents having an impact on the security of those products.

Manufacturers must submit these notifications through the [CRA Single Reporting Platform](#) (SRP) to the CSIRT designated as coordinator in the Member State determined under Article 14, generally the Member State where the manufacturer has its main establishment in the EU. The information is made available simultaneously to EU's cybersecurity agency (ENISA).

The reporting process generally consists of three stages:

Within 24 hours	Within 72 hours	Final report
of becoming aware of an actively exploited vulnerability or severe incident, an early warning must be submitted;	a more detailed vulnerability or incident notification must be submitted; and	for an actively exploited vulnerability, no later than 14 days after a corrective or mitigating measure has been made available; for a severe incident, within one month after the 72-hour notification.

Manufacturers must also **inform affected users**, and, where appropriate, all users, of an actively exploited vulnerability or severe incident and, where necessary, of any corrective or mitigating measures that users can take to mitigate its impact.

These requirements apply to in-scope products that have already been made available on the EU market, including products placed on the market before 11 December 2027.



The CRA reporting regime is separate from other applicable notification requirements. A single cybersecurity incident may trigger notification obligations under multiple legal frameworks, depending on the circumstances, including the GDPR, NIS2 or sector-specific legislation. Companies should therefore ensure that their incident-response procedures identify and appropriately coordinate potentially overlapping reporting obligations.



6 Existing Products, Updates and Substantial Modifications

Products with digital elements placed on the EU market before **11 December 2027** will generally not become subject to the CRA's substantive requirements solely because they are already on the market. However, such products may become subject to the CRA where, from 11 December 2027, they undergo a "**substantial modification**."

A substantial modification is a post-market change that affects the product's compliance with the essential cybersecurity requirements in Annex I, Part I, or modifies its intended purpose. The CRA and the Guidance distinguish substantial modifications from routine maintenance and security updates. For example, a security update intended to reduce cybersecurity risk that does not modify the product's intended purpose will generally not constitute a substantial modification. Similarly, minor changes such as visual enhancements or the addition of languages or pictograms will generally not constitute substantial modifications. By contrast, changes to a product's intended functions, type or performance may constitute a substantial modification, depending on their impact on the product's compliance and cybersecurity risk.



Companies should therefore consider incorporating a documented assessment of substantial modifications into their product-change and software-update processes, particularly for products that are continuously updated after launch.

7 Enforcement and Penalties

The CRA provides for enforcement by national market-surveillance authorities and requires Member States to establish effective, proportionate and dissuasive penalties for infringements of the CRA.

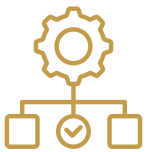
For non-compliance with the essential cybersecurity requirements set out in Annex I and the obligations set out in Articles 13 and 14, administrative fines may reach the higher of EUR 15 million or 2.5% of the undertaking's total worldwide annual turnover for the preceding financial year. Other categories of infringement are subject to lower maximum fines. The CRA also provides for corrective and restrictive measures in relation to non-compliant products, which may include requiring economic operators to take corrective action, withdraw products from the market or recall them. Accordingly, regulatory exposure under the CRA extends beyond financial penalties.



Companies should consider taking the following steps:

**Determine scope and exposure**

map relevant products and functionalities, including remote data-processing solutions, and identify any applicable exclusions or limitations;

**Determine the applicable compliance framework**

identify the relevant economic operator for each in-scope product, determine whether the product falls within any of the "important" or "critical" products categories and, where applicable, determine which conformity-assessment procedure applies;

**Conduct a legal gap analysis**

assess the company's existing contractual arrangements, product documentation, policies, procedures and governance framework against the CRA's applicable requirements, and identify any legal, regulatory or contractual gaps or overlapping requiring remediation or alignment;

**Establish CRA reporting readiness**

review and, where necessary, update incident-response and vulnerability-management procedures to ensure that potentially reportable actively exploited vulnerabilities and severe incidents can be identified, escalated and reported within the applicable CRA timelines, including coordination with other potentially applicable reporting obligations;

**Review existing processes and controls**

assess product development, cybersecurity, vulnerability-management, security-update, documentation and support processes against the CRA requirements;

**Build CRA-specific governance**

allocate responsibility across product, engineering, cybersecurity, legal and compliance functions, including ownership of reporting obligations and assessments of product changes; and

**Prepare for the implementation timeline**

prioritize the reporting requirements applicable from 11 September 2026 and plan for full compliance by 11 December 2027, including any required conformity assessments and technical documentation.



HERZOG'S TECHNOLOGY REGULATION DEPARTMENT

Herzog's Technology Regulation Department is a recognized market leader in its field.

The team is led by domain experts who possess a unique combination of **legal, technological** and **operational** expertise, and is uniquely positioned to advise a wide range of clients, including leading multinational technology companies as well as start-ups and vendors of disruptive technologies, on regulatory and compliance considerations across the digital ecosystem.

We understand that companies operating in digital environments face regulatory scrutiny that extends far **beyond one jurisdiction or discipline**. As our clients are often at the forefront of rapidly evolving markets, we recognize the impact that **global enforcement trends, platform rules and design-related compliance requirements** have on their products and operations. Our team maintains in-depth knowledge of the growing body of regulation, enforcement actions and industry standards that govern online interfaces, user journeys and commercial communications. This enables us to offer practical and holistic solutions for complex situations arising from innovative technologies and fast-moving regulatory expectations.

We assist our clients in ensuring they have appropriate measures in place, in order to manage their data protection and cyber risks and to respond effectively to incidents, while mitigating potential regulatory risks. Our assistance includes:

- Advice on the implementation of technical and organizational measures for risk mitigation and compliance;
- Compliance with evolving regulations and reporting obligations;
- Cyber corporate governance;
- Incident response plans and risk assessments;
- Data breach and cyber incidents response and management;
- Training for employees and management;
- Advice on sector specific cyber regulations (e.g., banking, financial institutions, critical infrastructure, cyber products);
- Compliance counseling and breach prevention;
- Advising on requirements in privacy and security policies;
- Cyber insurance policies;
- Data destruction and disposal practices;
- Agreements with security, forensic and incident response vendors;
- Vendor and supply chain management;
- Cyber and security due diligence and warranty negotiation for M&A and strategic transactions.

This document does not constitute an exhaustive legal opinion or regulatory overview of all applicable regulatory requirements regarding the topics addressed by it, but rather, only outlines the key issues arising from the regulatory requirements. Since we are not licensed to practice law outside of Israel, this document is intended to provide only a general background regarding this matter. This document should not be regarded as setting out binding legal advice, but rather a general overview which is based on our understanding of the practical interpretation of the applicable laws, regulations and industry guidelines.



Ariel Yosefi | Partner
Head of Technology Regulation
yosefia@herzoglaw.co.il



Ido Manor | Partner
Technology Regulation
manori@herzoglaw.co.il



Ruly Ber | Partner
Technology Regulation
berr@herzoglaw.co.il



Dan Shalev | Partner
Technology Regulation
shalevd@herzoglaw.co.il



Eden Lang | Partner
Technology Regulation
lange@herzoglaw.co.il



Dima Zalyalyeyev | Partner
Technology Regulation
zalyalyeyevd@herzoglaw.co.il



Or Noy | Partner
Technology Regulation
noyo@herzoglaw.co.il



Kevin David Gampel | Associate
Technology Regulation
gampelk@herzoglaw.co.il



On Dvori | Associate
Technology Regulation
dvorio@herzoglaw.co.il



Tal Habas | Associate
Technology Regulation
habast@herzoglaw.co.il



Zohar Malul | Associate
Technology Regulation
malulz@herzoglaw.co.il



Adaya Ziv-Kisos | Associate
Technology Regulation
Zivkisosa@herzoglaw.co.il



Liron Adar | Associate
Technology Regulation
adarl@herzoglaw.co.il



Omri Bar On | Associate
Technology Regulation
barono@herzoglaw.co.il



Eden Lapid | Associate
Technology Regulation
lapide@herzoglaw.co.il



Yuval Glazer | Associate
Technology Regulation
glazery@herzoglaw.co.il



Gal Mechtinger | Associate
Technology Regulation
mechtingerg@herzoglaw.co.il



Yoel Toledano | Associate
Technology Regulation
toledanoyo@herzoglaw.co.il



Clara Qubti | Associate
Technology Regulation
qubtyc@herzoglaw.co.il



Tal Schapiro | Associate
Technology Regulation
schapirot@herzoglaw.co.il



Roni Sharir | Intern
Technology Regulation
sharirR@herzoglaw.co.il



Korin Arbel | Pre-Intern
Technology Regulation
arbelk@herzoglaw.co.il



Tamar Oppenheim | Intern
Technology Regulation
oppenheimt@herzoglaw.co.il



Itay Siani | Intern
Technology Regulation
sianii@herzoglaw.co.il



Noya Schwartz | Law Student
Technology Regulation
schwartzn@herzoglaw.co.il



Max Shternberg | Law Student
Technology Regulation
shternbergm@herzoglaw.co.il