

CYBER RESILIENCE ACT PART ONE: COMPANIES PREPARE FOR FIRST NOTIFICATION OBLIGATIONS TO APPLY AS COMMISSION PUBLISHES IMPLEMENTATION GUIDANCE

Date: 19 August 2026

EU Corporate Alert

By: Sarah Pearce, Dr. Thomas Nietsch, Dr. Ulrike Elteste

On 20 November 2024, the European Union published Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act ([Regulation \(EU\) 2024/2847](#)) (the CRA). The CRA introduces the first EU-wide, horizontal legal framework imposing mandatory cybersecurity requirements on products with digital elements throughout their lifecycle. While most provisions of the CRA will apply from 11 December 2027, and only to products placed on the market in the European Economic Area (EEA) from that date, the notification obligations under Article 14 CRA apply before 11 September 2026 to all products with digital elements, regardless of when they were placed on the market. Manufacturers, importers and distributors placing connected products on the EU market should treat compliance planning as a near-term priority.

This opening instalment in our CRA series focuses on the first *notification obligations* which will apply from 11 September 2026. Later parts will examine the CRA's scope and core obligations in greater detail.

Article 14 imposes a stringent reporting regime requiring manufacturers to notify the competent cybersecurity agencies via a single reporting platform, of:

- Any actively exploited vulnerability in the product, and
- Any severe incident having an impact on the security of the product.

For each, manufacturers must submit an early warning within 24 hours of becoming aware of the event, a fuller notification within 72 hours, and (for vulnerabilities) a final report within 14 days of a corrective or mitigating measure becoming available, or (for incidents) a final report within one month of the initial incident notification. Manufacturers must also inform affected users of the vulnerability or incident and of any mitigating steps they should take.

WHAT COMPANIES SHOULD HAVE DONE ALREADY, OR SHOULD BE DOING NOW:

Determine the Extent to Which Any of Their Products Are in Scope of the CRA.

The CRA is a “horizontal” (not sector-specific) product safety law. It applies to products with digital elements distributed in the EEA. This includes most “smart” products and their components (with the notable exception of cars, which are subject to sector-specific laws), and it can also apply to standalone software that interacts with a product (including a user's computer).

Identify Which National Cyber Security Response Team (CSIRT) is Responsible to Receive Their Notifications.

Notices must be served to both The European Union Agency for Cybersecurity (ENISA) and the CSIRT competent for the manufacturer's main establishment in the EU via a single reporting platform. The reporting platform is not yet operational, but [ENISA has stated](#) that it will be operational in time. A list of the European CSIRTs is available [here](#).

For the purposes of the CRA, a manufacturer is considered to have its main establishment in the EU in the Member State where decisions related to the cybersecurity of its products with digital elements are predominantly taken. If such a Member State cannot be identified, the main establishment shall be considered as located in the Member State where the manufacturer has the highest number of employees in the EU.

If the manufacturer does not have a main establishment in the EU at all, it should report to the CSIRT in the Member State determined by applying the following criteria in strict order (i.e., each criterion applies only if the preceding one cannot be determined):

The Member State in which its authorised representative responsible for the highest number of products in scope of the CRA is established; or

The Member State in which the importer placing on the market the highest number of products in scope of the CRA is established; or

The Member State in which the distributor making available on the market the highest number of products with digital elements is established; or

The Member State in which the highest number of users of the manufacturer's in-scope products are located.

Establish Processes that Will Enable Them to Identify and Notify Exploited Vulnerabilities and Severe Incidents Within the Applicable Deadlines.

The notification obligation regarding actively exploited vulnerabilities applies if the manufacturer becomes aware of the active exploitation on or after 11 September 2026.

In practice, this means manufacturers should have in place: (i) a vulnerability and incident detection and triage process so that relevant events are identified quickly; (ii) a clear internal escalation path to whomever is responsible for CSIRT/ENISA reporting, given the 24-hour early warning deadline; (iii) a tracking process to meet the subsequent 72-hour and final report deadlines; and (iv) a process for identifying and notifying affected users of the vulnerability or incident and any mitigating steps they should take.

The information to be included in the notifications can be reviewed in advance on ENISA's website [here](#).

EU COMMISSION PUBLISHES BROADER IMPLEMENTATION GUIDANCE ON THE CRA

While most other obligations under the CRA will only apply from 11 December 2027, manufacturers whose products are in scope are already working on adjusting their compliance processes, including the paperwork for the CE certifications of their products and amending their contracts with suppliers.

On 27 July 2026, the EU Commission issued a nonbinding [Guidance](#) on the implementation of the CRA intended to address questions raised by stakeholders as they work through their preparation measures.

Significant parts of the Guidance are devoted to clarifications regarding the scope of the CRA:

- The Guidance confirms that the CRA applies to any individual tangible product with digital elements that is sold in the EEA after 11 December 2027. It does not matter that a product is of a type or series already being marketed prior to that date.
- By contrast, standalone software subject to the CRA is deemed to be “placed on the market” only once, on the date it is first made available in the EEA. If that first placing on the market occurred before 11 December 2027, the software does not fall within scope merely because further copies are distributed after that date since those later copies are not themselves treated as separate placings on the market. However, software that is a component of a tangible product is treated as a component of that product and follows the product's own “placing on the market” analysis.
- The Guidance explains when market actors using Free and Open Source Software are responsible for such software under the CRA.
- The Guidance discusses the term “substantial modification” of a product, which triggers obligations for the actor performing such modification.
- The Guidance explains when cloud solutions fall under the CRA and provides examples.

The document also provides guidance on how to perform the required risk assessments:

- The design and development related requirements of the CRA can and should be reasonably adapted for serial products designed and developed prior to December 2027 but sold after that date.
- There are indications that the requirements of the CRA could be eased if they conflict with interoperability requirements.

The EU Commission has also published (and is continuously updating) an FAQ document which can be found [here](#).

The German Federal Office of for Information Security BSI has also published an FAQ document in English with additional materials in German which can be found [here](#) and similar guidance is expected from other Member States in due course.

KEY CONTACTS



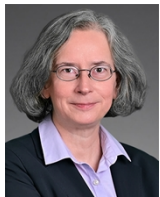
SARAH PEARCE
PARTNER

LONDON
+44.20.7360.8107
SARAH.PEARCE@KLGATES.COM



DR. THOMAS NIETSCH
PARTNER

BERLIN
+49.30.220.029.408
THOMAS.NIETSCH@KLGATES.COM



DR. ULRIKE ELTESTE
COUNSEL

FRANKFURT
+49.69.945.196.416
ULRIKE.ELTESTE@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.