REGUVARA / ENGLISH

Prepare your incident log and deadlines now

CRA incident reporting: a rapid response guide

For manufacturers of products with digital elements · triage questions, deadlines and first actions

Start with scope

If you manufacture a product with digital elements and make it available on the EU market, certain events may trigger reporting duties under Article 14 of the CRA. This guide helps your team prepare its response. Whether the CRA applies to your product and role must be assessed in context.

Is this reporting route likely to apply?

Check your role as manufacturer, whether the product has digital elements, and whether it is made available on the EU market. This guide covers manufacturers' Article 14 reporting duties; it is not a complete CRA scope assessment.

Which events may be reportable?

Actively exploited vulnerability
A vulnerability is actually exploited in an attack and affects the security of the product with digital elements. Not every discovered vulnerability meets this trigger.

Severe security incident
A severe incident affects the security of the product with digital elements. Not every IT incident at your company is automatically a CRA reportable event.

The clock starts when you become aware of the reportable event.

24 hours

Early warning: as soon as possible and no later than 24 hours.

72 hours

Notification with further information and an initial assessment, no later than 72 hours.

Final report

Vulnerability: no later than 14 days after a corrective measure is available. Severe incident: within one month of the 72-hour notification.

Where do manufacturers report?

Manufacturers submit one report through the CRA Single Reporting Platform (SRP). It is addressed to the CSIRT in the country of the manufacturer's main establishment; information is generally also made available to ENISA. The receiving CSIRT shares it with affected CSIRTs in other Member States.

Prepare before an incident

A small, clear readiness set saves valuable search time in the first hour:

- Name an incident lead and backup; agree how they can be reached outside office hours.
- Keep an up-to-date inventory of products, variants, software versions and EU markets.
- Set one internal channel for security findings and incident reports.
- List contacts for Product Security, Engineering, Legal/Compliance and Communications.
- Keep a shared event log ready for timestamps, decisions and owners.
- Agree in advance how to contain, correct and communicate an update.

First actions when an event occurs

Structure the response quickly, preserve evidence and actively track deadlines.

The first 60 minutes

01	Record when the organisation became aware: date, time, time zone, source and first recipient.
02	Activate a small core team and name one person accountable for reporting.
03	Make an initial classification: actively exploited vulnerability, severe incident or still unclear. Escalate promptly if uncertain.
04	Record the product, affected versions, possible impact, attack indicators and actions already taken. Preserve evidence.
05	Put the 24- and 72-hour deadlines on the calendar; prepare the SRP report and assign the final report as a follow-up.

Incident quick record

Case reference	Product / version(s)
First awareness (date, time, time zone)	Suspected event type
Reporting lead / backup	Affected markets / customers
Known impact and evidence	Immediate action / next update

Scope and limits

CRA reporting duties under Article 14 have applied since 11 September 2026 to manufacturers within scope. The specific assessment depends on the product, role, event and applicable exceptions. This free field guide is general information, not legal advice or a complete compliance or incident-response procedure. It does not submit a report or guarantee conformity. In a live event, check current law and the competent reporting route.

Official basis: Regulation (EU) 2024/2847, especially Articles 14 and 16 · European Commission guidance on CRA reporting obligations.

Open the EU Regulation · Open Commission guidance

Reguvara · Free CRA field guide · reguvara@outlook.com