



CRA - REPORTING OBLIGATION

2024/2847

Article 14

for Machine Tool Builders

starting from **SEP. 2026**

REPORTING TO OFFICIALS

Required for *all products in the market* (no matter how old)!

Any *vulnerability* that is *actively exploited*

ONCE AWARE

1. BEFORE 24hrs

Initial ENSIA/CSIRT notification with info on product, and in what EU countries it's used.

2. BEFORE 72hrs

Initial assessment:

- info on affected product
- general nature of the exploit & vulnerability
- Measures taken by MTB
- Measures that can be taken by the user

3. BEFORE 14 days (after fix)

Final report:

- Description of vulnerability
- Information on the malicious actor
- Details on security update and corrective measures

Severe incidents* impacting the product

ONCE AWARE

1. BEFORE 24hrs

Initial ENSIA/CSIRT notification:

- Suspected malicious activity?
- EU member states, where used

2. BEFORE 72hrs

Initial assessment:

- general info on incident
- nature of the incident
- Measures taken by MTB
- Measures that can be taken by the user

3. BEFORE 1 month (after 2.)

Final report:

- detailed description of incident
- type of threat or root cause
- applied and ongoing mitigation measures

* **Severe incidents** are security events that either:

- Disrupts a product's ability to keep critical data or functions available, authentic, intact or confidential
- Enables malicious code to run on the product or inside a user's network

PENALTIES

Up to **€15 Mio.**, or **2.5%** of total worldwide *revenue* of the previous year (whichever is higher).

(no fines for missing reporting deadlines, if a company has less than 50 employees and less than €10 Mio. revenue)

WHERE TO REPORT?

ENSIA/CSIRT will provide a central electronic reporting platform (not yet existing).

If your main office inside the EU:

- Report in this country.

If not, then:

- Report in the country, where you (or your dealer) sells most products.

(specific guidance will follow from the EU)

REPORTING TO USERS

You have to inform impacted users, else the officials will directly inform them.

VOLUNTARY REPORTING

You can voluntarily report to ENSIA any product vulnerabilities, cyber threats, security incidents, and near-misses.

For information purpose only, no legal advice.