CRA · NIS2 · GDPR

The first 24 hours: an early warning template for the CRA, NIS2 and the GDPR

Use this sheet the moment someone says “this vulnerability is being exploited” or “this incident looks significant”. It lists what each first message must contain, and what to keep ready for the follow-ups.

1. Start the clock

Write down the date, time and time zone at which you became aware. The CRA and NIS2 deadlines run from that moment, not from triage or from the end of the investigation.

Write down who decided, and the facts known at that time. You will be asked for them later.

2. CRA: an actively exploited vulnerability in your product (manufacturers)

Sent through ENISA’s single reporting platform to the CSIRT designated as coordinator. Reporting obligations have applied since 11 September 2026.

Early warning · 24 hours	That an actively exploited vulnerability is present in the product; where applicable, the Member States where you know the product has been made available. (Art. 14(2)(a))
Vulnerability notification · 72 hours	General information about the product; the general nature of the exploit and of the vulnerability; corrective or mitigating measures taken, and those users can take; how sensitive you consider the information. (Art. 14(2)(b))
Final report · 14 days after a fix or mitigation is available	A description of the vulnerability, with its severity and impact; where available, information about any malicious actor; details of the security update or other corrective measures. (Art. 14(2)(c))

> A severe incident having an impact on the security of your product follows the same 24-hour and 72-hour steps (with, in the early warning, whether it is suspected to be caused by unlawful or malicious acts) and a final report within one month of the incident notification (Art. 14(3) and (4)). Inform the impacted users, and where appropriate all users, about the vulnerability or incident and the measures they can take (Art. 14(8)).

3. NIS2: a significant incident (essential and important entities)

Sent to your CSIRT or competent authority, following your national transposition.

Early warning · 24 hours	Whether the incident is suspected of being caused by unlawful or malicious acts, and whether it could have a cross-border impact. (Art. 23(4)(a))
Incident notification · 72 hours	An update of the early warning; an initial assessment, with severity and impact; indicators of compromise, where available. (Art. 23(4)(b))
Intermediate report	On request of the CSIRT or competent authority. (Art. 23(4)(c))

Final report · one month after the notification	A detailed description, with severity and impact; the type of threat or root cause that likely triggered it; mitigation applied and ongoing; cross-border impact, where applicable. If the incident is still ongoing, a progress report instead, and the final report within one month of handling it. (Art. 23(4)(d) and (e))

4. GDPR: a personal data breach

Supervisory authority · 72 hours, where feasible	Unless the breach is unlikely to result in a risk to people's rights and freedoms. The nature of the breach, with the categories and approximate number of people and records concerned; the contact point; the likely consequences; the measures taken or proposed. Information can be given in phases. (Art. 33(1), (3), (4))
People concerned · without undue delay	When the breach is likely to result in a high risk to their rights and freedoms. (Art. 34)
Every breach, notified or not	Documented: facts, effects and remedial action. (Art. 33(5))

5. Fill in now

Aware at (date, time, time zone)
Decided by
Product or service, and versions
Applies: CRA vulnerability · CRA severe incident · NIS2 · GDPR · other (e.g. DORA: follow your financial supervisor's timelines, not covered here)
Suspected unlawful or malicious acts?
Cross-border impact? Member States
24-hour deadline at
72-hour deadline at
Sent at, by whom, reference received
Users informed (when, how)

In Jira: Clearlane CRA counts each CRA deadline from the recorded time of awareness, prepares every field for you to paste into ENISA's platform and keeps the exact text you sent. Clearlane Breach & Incident Reporting (coming soon) does the same for NIS2, the GDPR and DORA.
clearlaneapps.com/solutions/cyber

A working aid, not legal advice. Check the text of each regulation and the guidance of your national authority. References: Regulation (EU) 2024/2847 (CRA) Article 14; Directive (EU) 2022/2555 (NIS2) Article 23; Regulation (EU) 2016/679 (GDPR) Articles 33 and 34.