CRA Reporting Preparation Form under Article 14

Preparing notifications on ENISA's Single Reporting Platform under Regulation (EU) 2024/2847 (Cyber Resilience Act). Version 1.0, as of October 2026

This form helps manufacturers prepare the information for the three reporting stages under Article 14 CRA before they open ENISA's Single Reporting Platform (SRP). It reflects the information the Regulation requires, not the SRP input screen; field names there may differ and further fields may appear. The form does not replace legal advice. The text of the Regulation and the guidance of ENISA and the BSI are decisive. NIS2Compass accepts no liability for completeness, currency or legal certainty.

How to use it: in the header block, tick whether this concerns an actively exploited vulnerability (strand A) or a severe incident (strand B), and fill in only the matching part at each stage. According to the BSI, notifications on the SRP must be written in English, so write your entries in English straight away. Information already provided at an earlier stage does not have to be repeated (Article 14(2) and (4), points (b) and (c)).

Header block

Notification type	☐ A actively exploited vulnerability (Art. 14(1)) ☐ B severe incident (Art. 14(3))
Manufacturer (name, address)	
Member State of main establishment, i.e. where decisions on the cybersecurity of the products are predominantly taken (Art. 14(7))	
CSIRT designated as coordinator (in Germany: CERT-Bund at the BSI)	
Product concerned (name, type, versions, identifier)	
Vulnerability identifiers (CVE ID, EUVD ID), where available	
Time of becoming aware (date, time), starts the deadlines	
Who carried out the initial assessment and established awareness?	
Person reporting on the SRP (assigned representative, EU Login account with MFA) and deputy	
Notification identifier on the SRP (enter after the early warning)	

The deadlines run from the manufacturer becoming aware. According to Commission guidance C(2026) 5252 (Annex, paras. 213 and 214), that is the case once, after a prompt initial assessment, the manufacturer has a reasonable degree of certainty that a vulnerability is actively exploited or that a severe incident has occurred. Record the time and the basis of the assessment. If the Member State of the main establishment cannot be determined, the establishment with the highest number of employees in the Union applies; without a main establishment in the Union, the order is authorised representative, importer, distributor, users (Art. 14(7)). An incident is severe where it negatively affects or is capable of negatively affecting the ability of the product to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions, or where it has led or is capable of leading to the introduction or execution of malicious code in the product or in a user's systems (Art. 14(5)).

1. Early warning notification

Deadline: without undue delay, at the latest 24 hours after becoming aware (Art. 14(2)(a) and 14(4)(a))

A signal notification with the information known so far. Details follow in the 72-hour notification.

Strand A: actively exploited vulnerability	
Meaningful title of the notification (SRP field)	
Member States in which you know the product has been made available	
Short description (product concerned, what is being exploited)	

Strand B: severe incident	
Meaningful title of the notification (SRP field)	
Suspected unlawful or malicious act (mandatory)	☐ Yes ☐ No ☐ unclear
Member States in which you know the product has been made available	
Short description (product concerned, what was observed)	

2. Notification (72 hours)

Deadline: without undue delay, at the latest 72 hours after becoming aware (Art. 14(2)(b) and 14(4)(b))

Completes the same notification on the SRP. The Regulation calls it a vulnerability notification in strand A and an incident notification in strand B.

Strand A: actively exploited vulnerability	
General information about the product concerned	

General nature of the exploit and of the vulnerability	
Corrective or mitigating measures taken	
Corrective or mitigating measures that users can take	
How sensitive do you consider the notified information to be?	
Request delayed dissemination on justified cybersecurity-related grounds (Art. 16(2), second subparagraph; details in Delegated Regulation (EU) 2026/881)?	☐ Yes, grounds: ☐ No
Invoke particularly exceptional circumstances (PEC, Art. 16(2), third subparagraph)? Only basic information then goes to ENISA at first.	☐ a exploited only in the Member State of the receiving CSIRT ☐ b dissemination would be contrary to that Member State's essential interests ☐ c imminent high cybersecurity risk stemming from further dissemination ☐ no PEC

Strand B: severe incident	
Time of the incident, where known (SRP field)	
Nature of the incident	
Initial assessment of the incident	
Corrective or mitigating measures taken	
Corrective or mitigating measures that users can take	
How sensitive do you consider the notified information to be?	

3. Final report

Deadline A: no later than 14 days after a corrective or mitigating measure is available (Art. 14(2)(c)). Deadline B: within one month after submission of the incident notification (Art. 14(4)(c))

Once the final report is submitted, the notification can as a rule no longer be edited on the SRP. Check all information before submitting.

Strand A: actively exploited vulnerability	
Date from which the corrective or mitigating measure is available (starts the deadline)	
Description of the vulnerability, including its severity and impact	
Information on any malicious actor that has exploited or is exploiting the vulnerability, where available	
Details of the security update or other corrective measures made available	

Strand B: severe incident	
Detailed description of the incident, including its severity and impact	
Type of threat or root cause that is likely to have triggered the incident	
Applied and ongoing mitigation measures	

Additional blocks

Intermediate report (Art. 14(6)), only on request

The CSIRT initially receiving the notification may request an intermediate report on relevant status updates. Article 14(6) sets no deadline. Record any deadline stated in the request.

Date of the CSIRT's request	
Status update requested (free text)	

Informing users (Art. 14(8))

After becoming aware, the manufacturer informs the impacted users, and where appropriate all users, of the vulnerability or incident and, where necessary, of measures they can take, where appropriate in a structured, machine-readable format. If the manufacturer fails to do so in a timely manner, the CSIRT may inform the users itself.

Informed on (date, time)	
Users informed	☐ impacted users ☐ all users
Channel and format (e.g. security advisory, CSAF)	

Dual reporting check: NIS2 and GDPR

A CRA notification does not replace a NIS2 notification. If the same incident also affects your own operations as an essential or important entity, you also report under § 32 BSIG via the BSI portal, with its own deadline from your own awareness. According to the BSI, you can note a cross-reference to the other notification in each.

Significant security incident in your own operations (§ 2 no. 11, § 32 BSIG)?	☐ Yes, notify via the BSI portal ☐ No ☐ unclear
Incident ID in the BSI portal (cross-reference)	
Personal data affected (notification to the supervisory authority under Art. 33 GDPR)?	☐ Yes ☐ No ☐ unclear

Approval block (proof of deadlines)

Signature and time stamp per stage document internally that the deadline was met. Submit on the SRP only after approval.

Stage	Due by (date, time)	Approved by	Submitted on (date, time)
1 Early warning			
2 Notification (72 hours)			
Intermediate report			
3 Final report			

Basis: Regulation (EU) 2024/2847, Articles 14 and 16; Commission guidance C(2026) 5252 of 27 July 2026; ENISA, SRP FAQ and AR User Manual (September 2026); BSI page on the CRA Single Reporting Platform. Legal status 25 October 2026. Reporting obligation since 11 September 2026, also for products placed on the market before 11 December 2027 (Art. 69(3)). Fines under Article 64 only from 11 December 2027; no fines for micro and small enterprises for missing the 24-hour deadline (Art. 64(10)(a)). Explanations: nis2compass.de/en/blog/cra-reporting-art-14-vs-section-32-bsig