CRA-Melde-Vorbereitungsbogen nach Art. 14

Vorbereitung der Meldungen auf der ENISA Single Reporting Platform nach der Verordnung (EU) 2024/2847 (Cyber Resilience Act). Version 1.0, Stand: Oktober 2026

Dieser Bogen hilft Herstellern, die Angaben für die drei Meldestufen nach Art. 14 CRA vorzubereiten, bevor sie die ENISA Single Reporting Platform (SRP) öffnen. Er bildet die Pflichtangaben der Verordnung ab, nicht die Eingabemaske der SRP; dort können Felder anders heißen oder hinzukommen. Der Bogen ersetzt keine Rechtsberatung. Maßgeblich sind der Verordnungstext und die Hinweise von ENISA und BSI. NIS2Compass übernimmt keine Gewähr für Vollständigkeit, Aktualität oder Rechtssicherheit.

So gehen Sie vor: Kreuzen Sie im Kopfblock an, ob eine aktiv ausgenutzte Schwachstelle (Strang A) oder ein schwerwiegender Sicherheitsvorfall (Strang B) vorliegt, und füllen Sie je Stufe nur den passenden Teil aus. Meldungen auf der SRP sind laut BSI auf Englisch zu verfassen. Formulieren Sie die Einträge daher gleich auf Englisch. Angaben, die Sie in einer früheren Stufe schon gemeldet haben, müssen Sie nicht wiederholen (Art. 14 Abs. 2 und 4, jeweils Buchst. b und c).

Kopfblock

Meldungsart	☐ A aktiv ausgenutzte Schwachstelle (Art. 14 Abs. 1) ☐ B schwerwiegender Sicherheitsvorfall (Art. 14 Abs. 3)
Hersteller (Name, Anschrift)	
Mitgliedstaat der Hauptniederlassung, also wo die Entscheidungen zur Cybersicherheit der Produkte überwiegend fallen (Art. 14 Abs. 7)	
Als Koordinator benanntes CSIRT (in Deutschland: CERT-Bund im BSI)	
Betroffenes Produkt (Name, Typ, Versionen, Kennung)	
Kennungen der Schwachstelle (CVE-ID, EUVD-ID), soweit vorhanden	
Zeitpunkt der Kenntniserlangung (Datum, Uhrzeit), fristauslösend	
Wer hat die Erstbewertung vorgenommen und die Kenntnis festgestellt?	
Meldende Person auf der SRP (Assigned Representative, EU-Login-Konto mit MFA) und Vertretung	
Kennung der Meldung auf der SRP (nach der Frühwarnung eintragen)	

Die Fristen laufen ab der Kenntnis des Herstellers. Laut Leitlinie der EU-Kommission C(2026) 5252 (Anhang, Rn. 213 und 214) liegt sie vor, sobald er nach einer zügigen Erstbewertung mit hinreichender Gewissheit weiß, dass eine Schwachstelle aktiv ausgenutzt wird oder ein schwerwiegender Vorfall vorliegt. Halten Sie den Zeitpunkt und die Grundlage der Bewertung fest. Lässt sich der Mitgliedstaat der Hauptniederlassung nicht bestimmen, gilt die Niederlassung mit den meisten Beschäftigten in der EU; ohne Hauptniederlassung in der EU gilt die Reihenfolge Bevollmächtigter, Einführer, Händler, Nutzer (Art. 14 Abs. 7). Schwerwiegend ist ein Vorfall, wenn er die Fähigkeit des Produkts beeinträchtigt oder beeinträchtigen kann, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit sensibler oder wichtiger Daten oder Funktionen zu schützen, oder wenn er zum Einschleusen oder Ausführen von Schadcode im Produkt oder in den Systemen eines Nutzers geführt hat oder führen kann (Art. 14 Abs. 5).

1. Frühwarnung

Frist: unverzüglich, spätestens 24 Stunden nach Kenntniserlangung (Art. 14 Abs. 2 Buchst. a und Abs. 4 Buchst. a)

Signalmeldung mit den bis dahin bekannten Angaben. Einzelheiten folgen in der Meldung nach 72 Stunden.

Strang A: aktiv ausgenutzte Schwachstelle	
Aussagekräftiger Titel der Meldung (SRP-Angabe)	
Mitgliedstaaten, in denen das Produkt nach Ihrer Kenntnis bereitgestellt wurde	
Kurzbeschreibung (betroffenes Produkt, was ausgenutzt wird)	

Strang B: schwerwiegender Sicherheitsvorfall	
Aussagekräftiger Titel der Meldung (SRP-Angabe)	
Verdacht auf rechtswidrige oder böswillige Handlung (Pflichtangabe)	☐ Ja ☐ Nein ☐ unklar
Mitgliedstaaten, in denen das Produkt nach Ihrer Kenntnis bereitgestellt wurde	
Kurzbeschreibung (betroffenes Produkt, was beobachtet wurde)	

2. Meldung (72 Stunden)

Frist: unverzüglich, spätestens 72 Stunden nach Kenntniserlangung (Art. 14 Abs. 2 Buchst. b und Abs. 4 Buchst. b)

Ergänzt dieselbe Meldung auf der SRP. Strang A heißt in der Verordnung „Meldung von Schwachstellen“, Strang B „Meldung des Sicherheitsvorfalls“.

Strang A: aktiv ausgenutzte Schwachstelle	
Allgemeine Informationen zum betroffenen Produkt	
Allgemeine Art des Exploits und der Schwachstelle	
Ergriffene Korrektur- oder Risikominderungsmaßnahmen	
Maßnahmen, die Nutzer selbst ergreifen können	
Wie sensibel sind die gemeldeten Informationen aus Ihrer Sicht?	
Verzögerte Weitergabe aus gerechtfertigten cybersicherheitsbezogenen Gründen beantragen (Art. 16 Abs. 2 UAbs. 2; Näheres regelt die Delegierte VO (EU) 2026/881)?	☐ Ja, Gründe: ☐ Nein
Besonders außergewöhnliche Umstände (PEC, Art. 16 Abs. 2 UAbs. 3) geltend machen? Dann gehen zunächst nur Grundangaben an ENISA.	☐ a nur im Mitgliedstaat des empfangenden CSIRT ausgenutzt ☐ b Weitergabe widerspräche wesentlichen Interessen dieses Mitgliedstaats ☐ c unmittelbares hohes Cybersicherheitsrisiko durch die Weitergabe ☐ keine PEC

Strang B: schwerwiegender Sicherheitsvorfall	
Zeitpunkt des Vorfalls, soweit bekannt (SRP-Angabe)	
Art des Sicherheitsvorfalls	
Erste Bewertung des Vorfalls	
Ergriffene Korrektur- oder Risikominderungsmaßnahmen	
Maßnahmen, die Nutzer selbst ergreifen können	
Wie sensibel sind die gemeldeten Informationen aus Ihrer Sicht?	

3. Abschlussbericht

Frist A: spätestens 14 Tage, nachdem eine Korrektur- oder Risikominderungsmaßnahme verfügbar ist (Art. 14 Abs. 2 Buchst. c). Frist B: innerhalb eines Monats nach Übermittlung der Meldung des Sicherheitsvorfalls (Art. 14 Abs. 4 Buchst. c)

Nach dem Abschlussbericht ist die Meldung auf der SRP grundsätzlich nicht mehr bearbeitbar. Prüfen Sie die Angaben vor der Einreichung vollständig.

Strang A: aktiv ausgenutzte Schwachstelle	
Datum, ab dem die Korrektur- oder Risikominderungsmaßnahme verfügbar ist (fristauslösend)	
Beschreibung der Schwachstelle mit Schweregrad und Auswirkungen	
Informationen zum böswilligen Akteur, der die Schwachstelle ausgenutzt hat oder ausnutzt, soweit verfügbar	

Einzelheiten zum Sicherheitsupdate oder zu anderen bereitgestellten Korrekturmaßnahmen	

Strang B: schwerwiegender Sicherheitsvorfall	
Ausführliche Beschreibung des Vorfalls mit Schweregrad und Auswirkungen	
Art der Bedrohung oder zugrunde liegende Ursache, die den Vorfall wahrscheinlich ausgelöst hat	
Ergriffene und laufende Risikominderungsmaßnahmen	

Zusatzblöcke

Zwischenbericht (Art. 14 Abs. 6), nur auf Anforderung

Das CSIRT, das die Meldung zuerst erhält, kann einen Zwischenbericht über relevante Statusänderungen anfordern. Art. 14 Abs. 6 nennt keine Frist. Halten Sie eine in der Anforderung genannte Frist fest.

Datum der Anforderung durch das CSIRT	
Angeforderte Statusänderung (Freitext)	

Information der Nutzer (Art. 14 Abs. 8)

Nach Kenntnis informiert der Hersteller die betroffenen Nutzer, gegebenenfalls alle Nutzer, über die Schwachstelle oder den Vorfall und, falls nötig, über Maßnahmen, die sie selbst ergreifen können, wo angemessen in einem strukturierten, maschinenlesbaren Format. Informiert er nicht rechtzeitig, kann das CSIRT die Nutzer selbst informieren.

Informiert am (Datum, Uhrzeit)	
Kreis der Nutzer	☐ betroffene Nutzer ☐ alle Nutzer
Kanal und Format (z. B. Security Advisory, CSAF)	

Doppelmelde-Prüfung NIS2 und DSGVO

Eine CRA-Meldung ersetzt keine NIS2-Meldung. Trifft derselbe Vorfall auch Ihren eigenen Betrieb als besonders wichtige oder wichtige Einrichtung, melden Sie zusätzlich nach § 32 BSIG über das BSI-Portal, mit eigener Frist ab eigener Kenntniserlangung. Laut BSI können Sie in der jeweiligen Meldung einen Referenzhinweis auf die andere vermerken.

Erheblicher Sicherheitsvorfall im eigenen Betrieb (§ 2 Nr. 11, § 32 BSIG)?	☐ Ja, Meldung über das BSI-Portal ☐ Nein ☐ unklar
Vorfall-ID im BSI-Portal (Referenzhinweis)	
Personenbezogene Daten betroffen (Meldung an die Aufsicht nach Art. 33 DSGVO)?	☐ Ja ☐ Nein ☐ unklar

Freigabeblock (Fristnachweis)

Unterschrift und Zeitstempel je Stufe dokumentieren intern, dass die Frist eingehalten wurde. Erst nach Freigabe auf der SRP einreichen.

Stufe	Frist bis (Datum, Uhrzeit)	Freigegeben von	Eingereicht am (Datum, Uhrzeit)
1 Frühwarnung			
2 Meldung (72 Stunden)			
Zwischenbericht			
3 Abschlussbericht			

Grundlage: Verordnung (EU) 2024/2847, Art. 14 und 16; Leitlinien der EU-Kommission C(2026) 5252 vom 27.07.2026; ENISA, SRP-FAQ und AR User Manual (September 2026); BSI, Seite zur CRA Single Reporting Platform. Rechtsstand 25.10.2026. Meldepflicht seit 11.09.2026, auch für Produkte, die vor dem 11.12.2027 in Verkehr gebracht wurden (Art. 69 Abs. 3). Bußgelder nach Art. 64 erst ab 11.12.2027; für Kleinst- und Kleinunternehmen keine Bußgelder wegen versäumter 24-Stunden-Frist (Art. 64 Abs. 10 Buchst. a). Erläuterungen: nis2compass.de/de/blog/cra-meldepflicht-art-14-vs-32-bsig