REGUVARA · KOSTENLOSER PRAXISLEITFADEN

NIS2: Meldewege und Nachweise vorbereiten

Ein kostenloser Einstieg für Geschäftsleitung, IT/Informationssicherheit, Recht und Compliance. Mit Orientierung zum Anwendungsbereich, den zentralen Meldefristen und fünf ersten Arbeitsaufträgen.

Ziel dieses Leitfadens: in kurzer Zeit die richtigen Fragen sichtbar machen. Er entscheidet nicht verbindlich, ob eine konkrete Rechtseinheit unter NIS2 fällt.

1. Erst den Anwendungsbereich einordnen

- Tätigkeit, Dienst und Rechtseinheit den Sektoren in den Anhängen I und II der NIS2-Richtlinie zuordnen. Der Sektorname allein entscheidet die Einordnung nicht.
- Größe, verbundene Unternehmen, Diensttyp, kritische Einstufungen, Ausnahmen und besondere Regeln des betreffenden Mitgliedstaats prüfen. Bestimmte Einheiten oder Dienste können unabhängig von der üblichen Größenschwelle erfasst sein.
- Für jede potenziell betroffene Rechtseinheit Länder, Standorte, Dienste, zuständige Stelle, Registrierungs- und Kontaktpflichten sowie die Begründung dokumentieren.

2. EU-Meldeablauf bei einem erheblichen Sicherheitsvorfall

Schritt	EU-Basis nach Artikel 23	Vorbereitungsfrage
Frühwarnung	Ohne unangemessene Verzögerung, spätestens binnen 24 Stunden ab Kenntnis des erheblichen Vorfalls.	Wer startet die Uhr, wer entscheidet und welche Stelle ist zuständig?
Vorfallmeldung	Ohne unangemessene Verzögerung, spätestens binnen 72 Stunden ab Kenntnis; erste Bewertung von Schwere und Auswirkungen sowie Indikatoren, soweit verfügbar.	Wie werden Fakten, Zeitstempel und offene Punkte parallel gesammelt?
Zwischenbericht	Wenn CSIRT oder zuständige Behörde ihn anfordert.	Wer hält Statusänderungen fest und beantwortet Rückfragen?
Abschlussbericht	Grundsätzlich spätestens einen Monat nach der Vorfallmeldung. Bei weiter laufendem Vorfall: Fortschrittsbericht zu diesem Zeitpunkt und Abschlussbericht spätestens binnen eines Monats nach Bearbeitung.	Wer bestätigt den lokalen Termin und den vollständigen Inhalt?

Die Fristen beziehen sich auf einen erheblichen Vorfall und auf die Kenntnis davon. Für Vertrauensdiensteanbieter gilt eine besondere 24-Stunden-Regel für die Vorfallmeldung. Nationale Umsetzung, sektorale Vorgaben und weitere anwendbare EU-Rechtsakte zusätzlich prüfen.

ARBEITSBLATT

Vom Regeltext zum ersten Arbeitsablauf

Die EU-Richtlinie verlangt risikogerechte und verhältnismäßige technische, operative und organisatorische Maßnahmen. Diese Übersicht hilft, den ersten Verantwortlichenkreis zusammenzustellen.

3. Was Artikel 21 mindestens anspricht

Die Maßnahmen schützen die für Dienste genutzten Netz- und Informationssysteme einschließlich ihrer physischen Umgebung. Art und Umfang richten sich nach Risiko und Verhältnismäßigkeit.

Bereich	Beispiele für Arbeitsfragen
Risikoanalyse und Systemsicherheit	Welche Dienste, Systeme, Bedrohungen und Abhängigkeiten werden betrachtet? Wer aktualisiert die Risikobewertung?
Vorfallbehandlung	Wie werden Erkennung, Einstufung, Eindämmung, Eskalation, Beweissicherung und Nachbereitung organisiert?
Kontinuität und Krise	Sind Backups, Wiederherstellung, Krisenrollen und Wiederanlaufziele dokumentiert und erprobt?
Lieferkette	Sind direkte Lieferanten und Dienstleister samt kritischen Abhängigkeiten und Sicherheitsinformationen erfasst?
Sichere Beschaffung und Entwicklung	Wie werden Systeme sicher ausgewählt und gepflegt und Schwachstellen behandelt oder offengelegt?
Wirksamkeitsprüfung	Woran erkennt die Organisation, ob ihre Sicherheitsmaßnahmen wirksam sind?
Cyberhygiene und Schulung	Welche Basisschutzpraktiken und Schulungen sind vorgesehen und nachweisbar?
Kryptografie	Welche Regeln gelten für Kryptografie und - soweit angemessen - Verschlüsselung?
Personal, Zugriff und Anlagen	Wie werden Berechtigungen, Personalwechsel, Vermögenswerte und Zugriffe kontrolliert?
Authentisierung und Kommunikation	Wo sind MFA oder kontinuierliche Authentisierung, gesicherte Kommunikation und Notfallkommunikation angemessen?

4. Fünf sinnvolle erste Schritte

- Eine verantwortliche Person benennen, die Fragen zum Anwendungsbereich und offene Punkte koordiniert.
- Dienste, Rechtseinheiten, Systeme und direkte kritische Lieferanten erfassen.
- Management, Vorfallleitung, IT/Security, Recht/Compliance und Kommunikation mit Stellvertretungen benennen.
- Nationale zuständige Behörde, CSIRT, Registrierung, Meldekanal und etwaige sektorale Pflichten verifizieren.
- Eine kurze Übung durchführen: Vorfall erkennen, Kenntniszeitpunkt erfassen, Eskalation starten und Faktenlage aufbauen.

NIS2 gilt nicht automatisch für jedes Unternehmen. Die Einordnung hängt unter anderem von Tätigkeit, Größe, Rechtseinheit, Mitgliedstaat, Sonderfällen und sektoralen Regeln ab.

QUELLEN UND RECHTSSTAND

Primärquelle: Richtlinie (EU) 2022/2555, insbesondere Artikel 2-4, 20, 21 und 23 sowie Anhänge I-II. Die Änderung COM(2026) 13 final ist ein Vorschlag und kein geltendes Recht. Am 08.10.2026 wartete das Verfahren 2026/0012(COD) im Europäischen Parlament auf eine Ausschussentscheidung; ein Ausschussberichtsentwurf war am 24.09.2026 veröffentlicht. Nationale Umsetzung und sektorale Regeln wurden nicht für jedes Land einzeln geprüft.
NIS2 Directive (EUR-Lex) · European Commission FAQ · National transposition · EP procedure 2026/0012(COD) · COM(2026) 13 proposal