

Meldefristen auf einen Blick

NIS2, CRA, DORA, DSGVO und KI-VO im direkten Vergleich. Ein Sicherheitsvorfall kann mehrere Regime gleichzeitig auslösen. Diese Übersicht dient der ersten Orientierung: welche Uhr wann startet, was zu liefern ist und wer der Adressat ist. Die verbindliche Einordnung Ihres konkreten Vorfalls bleibt einer Einzelfallprüfung vorbehalten.

Regime	Rechtsgrundlage	Erstmeldung	Folgemeldung	Abschluss	Adressat
NIS2 / BSIG	§ 32 BSIG	24 h frühe Erstmeldung nach Kenntnis	72 h Meldung mit Erstbewertung	1 Monat Abschl ussmeldung	BSI-Meldeportal (live seit 06.01.2026)
CRA	Art. 14 VO (EU) 2024/2847, gilt seit 11.09.2026	24 h Frühwarnung bei aktiv ausgenutzter Schwachstelle oder schwerem Vorfall	72 h Detailmeldung	14 Tage (Schwachstelle) bzw. 1 Monat (Vorfall)	ENISA-Meldeplat tform und CERT-Bund
DORA	Art. 19 VO (EU) 2022/2554 i. V. m. RTS (EU) 2025/301	4 h nach Klassifizierung als schwerwiegend, spätestens 24 h nach Kenntnis	72 h Zwischenbericht	1 Monat Abschl ussbericht	BaFin
DSGVO	Art. 33, 34 DSGVO	72 h Meldung an die Aufsichtsbehörde nach Kenntnis	Nachmeldung bei schrittweiser Aufklärung zulässig	keine gesonderte Frist	Datenschutzaufsi cht; Betroffene unverzüglich (Art. 34)
KI-VO	Art. 73 KI-VO, anwendbar mit den Hochrisiko-Pflichten ab 02.12.2027	15 Tage; 2 Tage bei weitverbreitetem Verstoß oder KRITIS-Störung; 10 Tage bei Todesfall	auf Anforderung	Untersuchungs bericht nach Be hördenvorgabe	Marktüberwachu ngsbehörde

Alle Fristen laufen ab Kenntnis, nicht ab Ursache. Interne Eskalationszeit verkürzt deshalb direkt das verfügbare Meldefenster.

Sechs Praxisregeln für die Meldekette

Aus der Begleitung von Melde- und Aufsichtsfällen. Kurz, weil im Ernstfall niemand lange Dokumente liest.

1. Meldematrix vor dem Vorfall

Legen Sie je Regime fest: Auslöser, Frist, Adressat, Portal-Zugang, Formulierungsverantwortung, Freigabe. Ein Vorfall um 3 Uhr nachts ist der falsche Zeitpunkt, diese Fragen erstmals zu stellen.

2. Ein Vorfall, mehrere Regime

Prüfen Sie bei jedem Vorfall alle fünf Spuren parallel. Ein Ransomware-Angriff mit Kundendaten kann gleichzeitig NIS2- (24 h), DSGVO- (72 h) und bei Finanzunternehmen DORA-Meldungen (4 h) auslösen.

3. Portale und Zugänge vorher testen

BSI-Meldeportal, ENISA-Plattform und BaFin-Verfahren setzen eingerichtete Zugänge voraus, teils mit ELSTER-Organisationszertifikat. Die Einrichtung dauert Tage, die Frist läuft in Stunden.

4. Vorlagen halbfertig bereithalten

Erstmeldungen verlangen keine abschließende Analyse. Vorformulierte Templates mit Lückentext (Was, Seit wann, Betroffene Systeme, Erste Maßnahmen) sparen im Ernstfall die entscheidenden Stunden.

5. Kenntnis dokumentieren

Der Fristbeginn ist der Zeitpunkt der Kenntnis. Halten Sie fest, wer wann was wusste. Diese Dokumentation entscheidet später darüber, ob eine Meldung als fristgerecht gilt.

6. Die Anbieter-Meldung vertraglich befristen

Der Auftragsverarbeiter meldet Verletzungen an Sie, die Behördenmeldung bleibt bei Ihnen (Art. 33 Abs. 2 DSGVO). Das gesetzliche „unverzüglich“ wird erst belastbar, wenn der AVV eine konkrete Frist nennt, denn Ihre 72 Stunden laufen unabhängig davon.

Nächster Schritt

Unsere Regulatorik-Gap-Analyse zum Festpreis prüft Ihre Meldefähigkeit gegen alle fünf Regime und liefert eine einsatzbereite Meldematrix.

Kontakt: governance-first.de · Questax Systems GmbH, Heidelberg

Wichtiger Hinweis zur Nutzung dieses Dokuments. Dieses Dokument dient der ersten Orientierung und als initiale Vorabprüfung. Es stellt weder eine abschließende Bewertung noch eine Rechtsberatung im Sinne des Rechtsdienstleistungsgesetzes (RDG) dar und ersetzt keine einzelfallbezogene Prüfung durch qualifizierte Fachanwälte oder zertifizierte Compliance-Expertinnen und -Experten. Gesetzliche Fristen und Pflichten sind nach bestem Wissen zum angegebenen Stand wiedergegeben; maßgeblich sind stets die amtlichen Rechtstexte und die aktuelle Verwaltungspraxis der zuständigen Aufsichtsbehörden. Trotz sorgfältiger Erstellung wird keine Gewähr für Vollständigkeit, Richtigkeit und Aktualität übernommen. Eine Haftung der Questax Systems GmbH für Entscheidungen, die allein auf Grundlage dieses Dokuments getroffen werden, ist ausgeschlossen.