

Digitale Compliance in der EU

Praxisleitfaden

Massnahmen und Nachweise für neun EU-Rechtsakte

SCAI – Swiss Cyber AI | 8. Oktober 2026 | www.swisscyberai.org

Arbeitsgrundlage für Sicherheit, IT, Recht, Datenschutz, Einkauf und Fachbereiche. Geltungsbereich klären, Verantwortung zuweisen, dringende Lücken schliessen, Kontrollen testen und Nachweise sichern.

Den Leitfaden in drei Arbeitssitzungen nutzen

Sitzung	Aufgabe	Ergebnis
1 Abgrenzen 60 Minuten	Recht und Fachbereiche prüfen die Rechtsübersicht und Abgrenzungsfragen auf Seiten 2 und 3.	Freigegebener Geltungsbereich je Rechtsträger oder Dienst.
2 Zuweisen 90 Minuten	Verantwortliche ermitteln Lücken anhand der Seiten 4 bis 16 und der Lieferantenprüfung auf Seite 20.	Massnahmen, Zuständige, Fristen und Nachweisanforderungen.
3 Nachweisen Ein halber Tag	Meldungen üben, einen Dienst wiederherstellen und Nachweise stichprobenartig prüfen. Seiten 17 bis 23 nutzen.	Testergebnisse und finanzierter 90-Tage-Plan.

Schnell zum richtigen Abschnitt

Seiten	Arbeitsmaterial
2 bis 6	Verlinkte Rechtsübersicht, Geltungsbereich, Zuständigkeiten und gemeinsame Kontrollen
7 bis 16	NIS2 und praktische Checklisten zu allen neun Rechtsakten
17 bis 19	Vorfallbewältigung und Meldefristen
20 bis 23	Lieferantenprüfung, 90-Tage-Plan und wiederverwendbare Vorlagen
24	Termine und ergänzende amtliche Quellen

Lesehilfe: Rosa unterstrichene Verweise öffnen den Artikel oder Absatz auf EUR-Lex; Buchstaben sind in der Bezeichnung angegeben. «Dient» verknüpft eine Empfehlung mit ihrem rechtlichen Zweck, ohne Methode oder Ziel verbindlich zu machen. Zitate sind kurze Originalauszüge; die vollständige Vorschrift enthält die Bedingungen.

Pflichten nur im jeweiligen Geltungsbereich, für die betreffende Rolle und ab dem massgeblichen Datum anwenden. Nationale und sektorale Regeln ergänzen. Zuständigkeiten, Tests und 90-Tage-Plan sind Empfehlungen; der Leitfaden bescheinigt keine Compliance.

EU-Rechtsakte und amtliche Links

Den Rechtsakt in der letzten Spalte öffnen. Auf EUR-Lex die aktuelle konsolidierte Fassung, Änderungen und einschlägigen Durchführungsakte prüfen. Die folgenden Seiten zeigen die praktische Umsetzung.

Rechtsakt	Wann prüfen	Erstes Ergebnis	Amtlicher EU-Text
DSGVO	Verarbeitung personenbezogener Daten im räumlichen Geltungsbereich von Artikel 3.	Verzeichnis der Verarbeitungen und Datenflüsse.	Verordnung 2016/679 Art. 3, 5, 24, 28, 30 bis 35
NIS2	Erfasster Sektor oder Dienst, Grössenregeln und Ausnahmen. Nationale Umsetzung beachten.	Einstufung der Einrichtung und lokaler Meldeweg.	Richtlinie 2022/2555 Art. 2 bis 4, 20, 21, 23, 26
DORA	Aufgeführte Finanzunternehmen. Für benannte kritische IKT-Anbieter gelten eigene Regeln.	IKT-Rahmenwerk und Lieferantenregister.	Verordnung 2022/2554 Art. 2, 5 bis 16, 19, 24 bis 30
KI-VO	Anbieten oder Betreiben von KI im Geltungsbereich. Rolle und Verwendungszweck bestimmen die Pflichten.	KI-Inventar und Einstufung.	Verordnung 2024/1689 Art. 2 bis 6, 16, 26, 50, 53, 113
CRA	Erfasste Hardware- oder Softwareprodukte auf dem EU-Markt.	Produktabgrenzung und Prozess für Schwachstellenmeldungen.	Verordnung 2024/2847 Art. 2, 13, 14, 32, 69, 71; Anhang I
CER	Nach nationaler Umsetzung als kritisch eingestufte Einrichtungen.	Einstufungsnachweis und gefahrenübergreifender Risikoplan.	Richtlinie 2022/2557 Art. 6, 8, 12 bis 15
Data Act	Daten vernetzter Produkte, verbundene Dienste, Datenweitergabe oder Datenverarbeitungsdienste.	Datenzugangsprozess und getesteter Cloud-Ausstieg.	Verordnung 2023/2854 Art. 1 bis 5, 13, 23 bis 31, 50
eIDAS	Elektronische Identität, Signaturen, Siegel und Vertrauensdienste; rollenabhängige Pflichten.	Signaturrichtlinie und Prüfung des Vertrauensdienstes.	Verordnung 910/2014 Geändert durch 2024/1183
DSA	Vermittlungsdienste für Nutzer in der EU; abgestufte Pflichten je nach Art und Grösse.	Diensteinstufung und Meldeverfahren.	Verordnung 2022/2065 Art. 2, 11 bis 18, 19 bis 32, 33

KI-Verordnung zusammen mit Verordnung (EU) 2026/1744 lesen; diese ändert Fristen und Pflichten. Die eIDAS-Konsolidierung enthält die Änderung zur europäischen digitalen Identität. Für NIS2 und CER zusätzlich zum EU-Link das nationale Recht erfassen.

Rechtsgrundlagen [Änderung der KI-VO 2026/1744](#) | [eIDAS-Änderung 2024/1183](#)

Anwendbarkeit bestimmen

Für jeden Rechtsträger und jede relevante Tätigkeit den Geltungsbereich dokumentieren. Eine Konzernbewertung reicht nicht. Ein Schweizer Hauptsitz klärt nicht die Lage von EU-Tochtergesellschaften, Produkten auf dem EU-Markt oder Diensten für die EU.

In dieser Reihenfolge fragen	Zu dokumentieren	Weiter zu
1 Welcher Rechtsträger und welche Tätigkeit?	Juristischer Name, Land, Niederlassung, Dienst, Produkt, Kunden und EU-Bezug. NIS2 Art. 26 · DSGVO Art. 3 · DSA Art. 2(1)	Vorlage auf Seite 22 nutzen.
2 Werden personenbezogene Daten verarbeitet?	Rolle als Verantwortlicher oder Auftragsverarbeiter, betroffene Personen und räumliche Prüfung nach Artikel 3. DSGVO Art. 3 · DSGVO Art. 4(7) · DSGVO Art. 4(8)	DSGVO auf Seite 9.
3 Gehört die Einrichtung zu einem erfassten Sektor?	Tatsächliche Dienste, Kategorie in NIS2-Anhang I oder II, EU-Grössenberechnung, Ausnahmen und nationales Recht. NIS2 Art. 2 · NIS2 Anhang I · NIS2 Anhang II	NIS2 auf Seiten 7 und 8.
4 Ist es ein reguliertes Finanzunternehmen?	Genaue Kategorie nach Artikel 2, Ausnahmen und gegebenenfalls vereinfachtes Regime. DORA Art. 2 · DORA Art. 16	DORA auf Seite 10.
5 Wird KI angeboten oder eingesetzt?	Zweck, Anbieter-/Betreiberrolle und Prüfung auf Verbote, hohes Risiko, Transparenz und GPAI. KI-VO Art. 2 · KI-VO Art. 5 · KI-VO Art. 6	KI-Verordnung auf Seite 11.
6 Werden digitale Produkte verkauft?	Hersteller-, Einführer- oder Händlerrolle, Produktabgrenzung, Ausnahmen und EU-Inverkehrbringen. CRA Art. 2 · CRA Art. 3 · CRA Art. 32	CRA auf Seite 12.
7 Liegt eine Mitteilung zur kritischen Einrichtung vor?	Einstufung, Eingangsdatum, erfasster Dienst und sektorale Ausnahmen. CER Art. 6(3) · CER Art. 8	CER auf Seite 13.
8 Welche Daten- oder Onlinedienste bestehen?	Vernetzte Produkte, Cloud- und Vertrauensdienste, Hosting für Nutzer oder Marktplatzfunktionen. Data Act Art. 1 · eIDAS Art. 2 · DSA Art. 3(g)	Seiten 14 bis 16.

Eine überprüfbare Schlussfolgerung freigeben

Vier Ergebnisse verwenden: gilt jetzt; gilt ab Datum; gilt nicht, mit Begründung; ungeklärt, mit Prüfer und Frist. Tatsachen und Rechtsgrundlage beifügen.

Lieferantenverträge begründen eigene Pflichten. Ein regulierter Kunde kann vertragliche Vorgaben verlangen, auch wenn der Lieferant nicht unmittelbar unter das Gesetz fällt. Das Verhältnis DORA/NIS2 für das betroffene Finanzunternehmen und die jeweiligen Pflichten prüfen.

Bei Änderungen neu prüfen

- Neues Land, Akquisition, neuer Dienst, neues Produkt, KI-Zweck, Kundensegment oder Behördenmitteilung.
- Wesentliche Änderung von Grösse, Auslagerung, Markenauftritt, Produkt oder Rechtslage.

Rechtsgrundlagen [NIS2 Art. 2 bis 4](#) | [DSGVO Art. 3](#) | [DORA Art. 1 und 2](#)

Verantwortung und Abschlusskriterien festlegen

Die Leitung bleibt für ihre gesetzlichen Pflichten verantwortlich. Der CISO koordiniert Sicherheit; Fachbereiche, Datenschutz, Recht und Produktverantwortliche übernehmen ihre Aufgaben. Rollen durch konkrete Namen ersetzen.

Rolle	Praktische Verantwortung	Abschlussnachweis
Sponsor in der Geschäftsleitung	Geltungsbereich, Prioritäten, Ressourcen und wesentliche Risikoentscheide genehmigen. Überfällige kritische Massnahmen klären. Dient: NIS2 Art. 20(1) · DORA Art. 5(2)	Datierte Entscheide, Budget und Nachverfolgung.
Recht oder Compliance	Rollen, nationale Regeln, Behördenwege und Fristen klären; Rechtsregister pflegen. Dient: NIS2 Art. 2 · NIS2 Art. 23 · DSGVO Art. 24(1)	Geprüfte Abgrenzungs- und Meldeunterlagen.
CISO und Sicherheitsbetrieb	Cyberkontrollen, Erkennung, Reaktion und Wirksamkeitsprüfung koordinieren. Abdeckungslücken erfassen. Dient: NIS2 Art. 21(1) · DORA Art. 5(2)(c)	Kontrollverantwortliche, Tests und Vorfallakten.
CIO und Dienstverantwortliche	Assets, Zugänge, Konfiguration, Mängelbehebung und Wiederherstellung betreuen. Dient: DORA Art. 8(1) · DORA Art. 9(4) · DORA Art. 12(1)	Abdeckungsnachweise und Wiederherstellungsergebnisse.
Datenschutzleitung und DSB	Die Datenschutzleitung betreibt das Programm; ein bestellter Datenschutzbeauftragter berät und überwacht unabhängig. Dient: DSGVO Art. 24(1) · DSGVO Art. 38 · DSGVO Art. 39(1)	Verarbeitungsunterlagen, Beratung und Betroffenenanfragen.
Produkt- oder KI-Verantwortliche	Produktlebenszyklus oder KI-Verwendungszweck, Freigaben, Überwachung und Support verantworten. Dient: CRA Art. 13 · KI-VO Art. 16 · KI-VO Art. 26	Einstufung, Freigabe und Änderungshistorie.
Einkauf und Lieferantenverantwortliche	Sorgfaltsprüfung durchführen, Verträge sichern, Lieferanten überwachen und Ausstiegspläne pflegen. Dient: NIS2 Art. 21(2)(d) · DORA Art. 28	Freigegebene Lieferantenakte und getesteter Ausstieg.
Unabhängige Prüfung	Nachweise möglichst unabhängig vom Kontrollbetrieb stichprobenartig prüfen; Abschluss bestätigen. Dient: NIS2 Art. 21(2)(f) · DORA Art. 6(6)	Feststellungen, Nachtests und Abschlussentscheide.

Klare Abschlusskriterien anwenden

- Geltungsbereich, verantwortliche Person und Betriebsverfahren der Kontrolle sind dokumentiert.
- Die Umsetzung deckt den vorgesehenen Bestand ab; Ausnahmen sind sichtbar und genehmigt.
- Ein datierter Test belegt das Ergebnis; Fehler haben Massnahmen und Fristen.
- Der Nachweislink funktioniert und zeigt Einrichtung, System, Zeitraum und Prüfer.

Kurze monatliche Überprüfung durchführen

Neue Geltungsbereiche, überfällige Hochrisikomassnahmen, fehlgeschlagene Tests und Meldebereitschaft prüfen. Bei Finanzierungsbedarf oder Risikoakzeptanz einen konkreten Leitungsentscheid einholen. Das Gesamtprogramm als empfohlenen Rhythmus mindestens quartalsweise prüfen.

Rechtsgrundlagen [NIS2 Art. 20](#) | [DORA Art. 5](#) | [DSGVO Art. 24 und 38](#)

Gemeinsame Sicherheitsbasis umsetzen

Vorhandene NIST- oder andere geeignete Kontrollen nutzen. Die folgenden Massnahmen sind praktische Ausgangspunkte, keine EU-Zertifizierungsscheckliste. Frequenzen und Ziele risikobasiert festlegen; strengere Rechts- oder Vertragsvorgaben beachten.

Kontrolle und Massnahme	Zuständigkeit empfohlen	Nachweisstichprobe
01 Kritische Dienste, IT, Cloud, OT, Daten und Abhängigkeiten inventarisieren. Erkannte Bestände mit dem Register abgleichen. Dienst: NIS2 Art. 21(2)(i) · DORA Art. 8(1)	Dienstverantwortliche	Nicht verwaltete Assets und Abhängigkeitsübersicht.
02 Starke Authentisierung und minimale Rechte durchsetzen. Administratorkonten trennen; Notfallzugänge steuern. Dienst: NIS2 Art. 21(2)(i)-(j) · DORA Art. 9(4)(c)-(d)	Identitätsteam	Anmeldung, privilegierte Rechte und Austrittsentzug testen.
03 Schwachstellen nach Ausnutzung, Exposition und Dienstwirkung priorisieren. Ausnahmen befristen. Dienst: NIS2 Art. 21(2)(e) · DORA Art. 9(4)(f)	IT und OT	Dringenden Befund von der Behebung bis zum Nachtest prüfen.
04 Sichere Konfiguration und Endgeräteschutz umsetzen. Server und nicht mehr unterstützte Geräte in Lückenberichte aufnehmen. Dienst: DORA Art. 9(2)-(3) · NIS2 Art. 21(1)	IT-Betrieb	Abdeckungsbericht und getestete Reaktion auf Erkennung.
05 Kritische Systeme segmentieren und Fernzugänge schützen. Lieferantenzugänge und Notfallisolation testen. Dienst: DORA Art. 9(4)(b) · NIS2 Art. 21(1)	Netzwerk und OT	Erlaubte Verbindungen testen; genehmigte Isolationsübung.
06 Relevante Sicherheitslogs sammeln, Alarme überwachen und Reaktion ausserhalb der Bürozeiten sicherstellen. Dienst: DORA Art. 10(1)-(3) · NIS2 Art. 21(2)(b)	Sicherheitsbetrieb	Nachweis von Erkennung bis Reaktion; Eskalation beantwortet.
07 Backups vor Kompromittierung der Produktion schützen. Einen vollständigen Geschäftsdienst wiederherstellen. Dienst: NIS2 Art. 21(2)(c) · DORA Art. 12(1)-(3)	Dienstverantwortliche	Tatsächliche Wiederherstellungszeit, Datenintegrität und Fachfreigabe.
08 Kritische Lieferanten, Konzentration und Unterauftragnehmer bewerten; schnelle Vorfallohilfe vereinbaren. Dienst: NIS2 Art. 21(2)(d) · DORA Art. 28(4) · DORA Art. 30	Einkauf	Risikobewertung, Vertrag und getesteter Kontaktweg.
09 Sensible Daten durch Zugriffsregeln, Verschlüsselung und geregelte Aufbewahrung schützen. Dienst: DSGVO Art. 5(1)(e)-(f) · DSGVO Art. 32(1)(a) · NIS2 Art. 21(2)(h)	Datenverantwortliche	Zugriffsstichprobe, Schlüsselwiederherstellung und Löschnachweis.
10 Personal und Leitung schulen; Vorfälle, Kontinuität und gesetzliche Meldungen üben. Dienst: NIS2 Art. 20(2) · NIS2 Art. 21(2)(g) · DORA Art. 13(6)	HR und CISO	Rollengerechte Schulung und abgeschlossene Übungsmassnahmen.

Priorisieren und nicht auf das Gesamtprogramm warten

Exponierte privilegierte Zugänge, ausgenutzte Schwächen, fehlende kritische Backups und unbrauchbare Meldewege sofort eskalieren. Übergangsschutz und dauerhafte Behebung zuweisen. Ein genehmigter Plan allein senkt die Exposition nicht.

Rechtsgrundlagen [NIS2 Art. 21](#) | [DSGVO Art. 32](#) | [DORA Art. 6 bis 14](#)

Kontrollen mit Pflichten und Entscheidungen verknüpfen

Gemeinsame Nachweise wiederverwenden, aber jede Rechtsanforderung und Restlücke getrennt erfassen. Reifegrad oder Zertifikat sind im jeweiligen Umfang unterstützende Nachweise, kein automatischer Compliance-Beleg.

Gemeinsame Aufgabe	Unterstützte Rechtsgrundlagen	Unterschiede sichtbar halten
Risikobewertung	NIS2 Art. 21(2)(a) · DORA Art. 6(1) · DSGVO Art. 35(1) · CER Art. 12 · KI-VO Art. 9	Dienstrisiken, Personenschäden, physische Resilienz und KI-Risiken haben unterschiedliche Prüfkriterien.
Zugang und Wiederherstellung	DSGVO Art. 32(1)(b)-(c) · NIS2 Art. 21(2)(c) · DORA Art. 9 · DORA Art. 12	Systembestand, Geschäftswiederanlauf und Nachweiszeitraum prüfen.
Sichere Entwicklung	CRA Art. 13(1)-(2) · CRA Anhang I · NIS2 Art. 21(2)(e) · KI-VO Art. 9	Produktkonformität und KI-Rollenpflichten separat prüfen.
Lieferantenprüfung	DSGVO Art. 28(3) · NIS2 Art. 21(2)(d) · DORA Art. 28 · DORA Art. 30 · Data Act Art. 25	Auftragsverarbeitung, Finanz-IKT-Verträge und Wechselrechte unterscheiden sich.
Vorfallbewältigung	DSGVO Art. 33 · DSGVO Art. 34 · NIS2 Art. 23 · DORA Art. 19 · CRA Art. 14 · CER Art. 15	Auslöser, verpflichtete Einrichtung, Behörde, Frist und Meldeinhalt unterscheiden sich.

Risikoentscheide umsetzbar machen

Szenario, betroffenen Dienst und Personen, Schutzmassnahmen, plausible Folgen und Behandlung erfassen. Zuständigkeit und Frist festlegen. Einen Test zur Risikoreduktion definieren. Risiken eskalieren, die nicht finanziert oder rechtmässig akzeptiert werden können.

Ausnahmen befristen

Ausnahmen brauchen Umfang, Grund, Ersatzkontrolle, Genehmigung, Ablaufdatum und Abschlusstest. Risikoakzeptanz hebt keine Rechtspflicht auf. Recht muss die Zulässigkeit der Übergangslösung prüfen.

Beispiel einer belastbaren Zuordnung

Ein Test belegt, dass Anwendung A innerhalb des vereinbarten Ziels wiederhergestellt wird. Den passenden Verfügbarkeits- und Wiederherstellungspflichten zuordnen. Fehlende Lieferantenabhängigkeiten oder ungetestete Identitätsdienste bleiben offene Lücken; nicht das gesamte Gesetz als erfüllt markieren.

Prüfung vor Änderungen

Vor neuem Dienst, Lieferanten, KI-Einsatz oder Produktfreigabe: Geltungsbereich neu prüfen, Risiken aktualisieren, Meldungen oder Konformitätsschritte klären, Kontrollen testen und Fachfreigabe dokumentieren. Bei geändertem Verwendungszweck wiederholen.

Rechtsgrundlagen [NIS2 Art. 21](#) | [DSGVO Art. 25 und 35](#) | [CRA Anhang I](#)

NIS2 Geltungsbereich und Leitung

Geltung je Rechtsträger und Dienst bestimmen. Nationales Umsetzungsrecht anwenden; bei gesetzlicher Selbstprüfung oder Registrierung nicht auf ein Behördenschreiben warten.

Aus dem Gesetz „Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen“ [NIS2 Art. 20\(1\)](#)

Die Genehmigung durch die Leitung steht ausdrücklich im EU-Text; nationales Recht umsetzen.

Schritt	Massnahme	Benötigtes Ergebnis
1 Tätigkeit zuordnen	Tatsächliche Dienste den Anhängen I oder II und nationalen Kategorien zuordnen. Dazu zählen Energie, Verkehr, Gesundheit, Wasser, digitale Infrastruktur, IKT-Dienstemanagement und bestimmte Fertigungsbereiche. NIS2 Art. 2(1) · NIS2 Anhang I · NIS2 Anhang II	Begründung für Sektor und Dienst mit genauer Vorschrift.
2 Grösse berechnen	EU-Grössenregeln einschliesslich relevanter Partner- und verbundener Unternehmen anwenden. Beschäftigte und Finanzdaten erfassen. Ausnahmen für kleinere Einrichtungen prüfen. NIS2 Art. 2(1)-(2)	Von Recht geprüfte Berechnung und Ausnahmen.
3 Einrichtung einstufen	Wesentlich oder wichtig nach Artikel 3 und nationalem Recht bestimmen. Besondere Einstufungen und grenzüberschreitende Zuständigkeit prüfen. NIS2 Art. 3(1)-(2) · NIS2 Art. 26	Einstufung und zuständige Behörde.
4 Registrierung klären	Lokale Fristen, Registrierungsdaten, Portalzugang und Änderungsmeldungen klären. Verantwortliche Person und Stellvertretung benennen. NIS2 Art. 3(4) · NIS2 Art. 27(2)-(3)	Eingangsbestätigung oder dokumentierter Grund für fehlende Registrierungspflicht.
5 Leitung einbinden	Die Leitung genehmigt und überwacht die Risikomassnahmen und absolviert erforderliche Schulungen. Entscheide und Ressourcen dokumentieren. NIS2 Art. 20(1)-(2)	Protokolle, Schulungsnachweise und Massnahmenzuständige.
6 Meldungen vorbereiten	Erheblichkeitskriterien und Meldefristen festlegen. Für bestimmte digitale Anbieter gilt Verordnung 2024/2690. NIS2 Art. 23(3)-(4) · 2024/2690 Art. 3	Lokales Verfahren, getesteter Kanal und Vorfalübung.

Praktische Einstufungsfragen

- Betreiben wir selbst einen erfassten Dienst oder kaufen wir ihn nur ein?
- Gehört die Fertigung zu einer konkret aufgeführten Kategorie?
- Ändern eine Kleinunternehmensausnahme, kritische Einstufung oder ein Sektorgesetz das Ergebnis?

Überschneidungen: Bei DORA-Finanzunternehmen das sektorale Verhältnis nach NIS2-Artikel 4 prüfen. DSGVO sowie Produkt- und weitere Pflichten weiterhin berücksichtigen.

Rechtsgrundlagen [NIS2 Art. 2 bis 4 und 20](#) | [Durchführungsregeln für digitale Sektoren](#)

NIS2 Checkliste zur Umsetzung

Artikel 21 verlangt verhältnismässige technische, operative und organisatorische Massnahmen. Die zehn Bereiche dienen als Vollständigkeitsprüfung; nationale Vorgaben und Risikobewertung bestimmen die konkrete Umsetzung.

Aus dem Gesetz „Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmassnahmen im Bereich der Cybersicherheit“ [NIS2 Art. 21\(2\)\(f\)](#)
 Testergebnisse und Korrekturmassnahmen aufbewahren, nicht nur Richtlinien.

Bereich nach Artikel 21	Praktische Massnahme	Nachweis
Risikoanalyse und Sicherheitsrichtlinie	Dienstbezogene Risikobewertung und anwendbare Sicherheitsrichtlinie genehmigen. NIS2 Art. 21(2)(a)	Aktuelle Bewertung, Freigabe und Behandlungsplan.
Vorfallbewältigung	Triage, Reaktionsbefugnisse, Eindämmung und Meldeentscheide definieren. NIS2 Art. 21(2)(b)	Ablaufplan, Übung und Vorfälle.
Kontinuität und Krisenmanagement	Wiederherstellungsziele festlegen; Backups schützen und Wiederherstellung testen. NIS2 Art. 21(2)(c)	Wiederherstellungsergebnisse und Krisenübung.
Lieferkettensicherheit	Direkte Lieferanten und Dienstleister bewerten; relevante Schwachstellen und sichere Verfahren berücksichtigen. NIS2 Art. 21(2)(d)	Lieferantenregister, Entscheide und Verträge.
Beschaffung und Entwicklung	Sicherheit in Design, Änderungen, Wartung sowie Behandlung und Offenlegung von Schwachstellen integrieren. NIS2 Art. 21(2)(e)	Freigabenachweise und Schwachstellenliste.
Wirksamkeitsbewertung	Prüfen, ob Kontrollen im gesamten beanspruchten Umfang funktionieren. NIS2 Art. 21(2)(f)	Stichproben, Fehler und Nachtests.
Cyberhygiene und Schulung	Nutzer und Leitung nach Rolle und aktuellen Risiken schulen. NIS2 Art. 21(2)(g)	Schulungsnachweise und Lernkontrollen.
Kryptografie	Einsatz der Verschlüsselung definieren; Schlüssel und Wiederherstellung verwalten. NIS2 Art. 21(2)(h)	Standard, Schlüsselzuständigkeit und getestete Wiederherstellung.
Personal, Zugriffe und Assets	Eintritte, Wechsel, Austritte, privilegierte Rechte und Asset-Verantwortung steuern. NIS2 Art. 21(2)(i)	Zugriffsprüfung und Bestandsabgleich.
Authentisierung und Kommunikation	Wo angemessen MFA oder kontinuierliche Authentisierung und sichere Kommunikation einsetzen. NIS2 Art. 21(2)(j)	Konfiguration, Ausnahmen und Test des Notfallkanals.

Drei Nachweise im ersten Monat

- Bei Austritt werden alle Zugänge, auch privilegierte und externe, innerhalb des genehmigten Ziels entzogen.
- Ein kritischer Dienst ist samt Identitäts-, Netzwerk- und Lieferantenabhängigkeiten wiederherstellbar.
- Das Vorfalldteam erreicht den richtigen Behördenkanal und erstellt rechtzeitig eine Frühwarnung.

Verordnung 2024/2690 enthält Detailanforderungen für bestimmte digitale Einrichtungen. Sie gilt nicht automatisch für alle NIS2-Sektoren.

Rechtsgrundlagen [NIS2 Art. 21](#) | [Verordnung 2024/2690](#)

DSGVO Praxischeckliste

Verantwortliche und Auftragsverarbeiter getrennt bewerten. Beschäftigten- und Geschäftskontaktdaten sind personenbezogen; B2B ist keine generelle Ausnahme. Der Verantwortliche trägt die Rechenschaftspflicht; ein bestellter Datenschutzbeauftragter (DSB) berät und überwacht.

Aus dem Gesetz „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können“ [DSGVO Art. 5\(2\)](#)

Nachweise jeder Kontrolle leicht auffindbar ablegen.

Massnahmen und Nachweise

Massnahme	Zuständigkeit empfohlen	Aufzubewahrende Nachweise
Zwecke, Daten, Personen, Empfänger und Aufbewahrung erfassen. Rechtsgrundlagen und nötige Bedingungen für besondere Datenkategorien dokumentieren. DSGVO Art. 5(1) · DSGVO Art. 6 · DSGVO Art. 9 · DSGVO Art. 30	Fachbereich und Datenschutz	Verarbeitungsverzeichnis, Rechtsgrundlage und Datenflussübersicht.
Klar informieren und nur notwendige Daten erheben. Aufbewahrung und wirksamen Lösprozess definieren. DSGVO Art. 5(1)(c)-(e) · DSGVO Art. 13 · DSGVO Art. 14	Datenverantwortliche	Veröffentlichte Hinweise und geprüfte Löschstichprobe.
Verträge nach Artikel 28 mit Auftragsverarbeitern abschliessen. Unterauftragsverarbeiter, internationale Übermittlungen und Schutzmassnahmen prüfen. DSGVO Art. 28(2)-(3) · DSGVO Art. 44 · DSGVO Art. 46	Recht und Einkauf	Auftragsverarbeitungsverträge und Transferbewertung.
Risikogerechte Sicherheit umsetzen. Bedarf einer Datenschutz-Folgenabschätzung (DSFA) prüfen; vor risikoreicher Verarbeitung abschliessen. DSGVO Art. 32(1) · DSGVO Art. 35(1)	CISO und Datenschutz	Kontrolltests, DSFA und Behandlungsentscheide.
Betroffenen anfragen sicher bearbeiten. Einmonatsfrist und zulässige Verlängerung verfolgen; Verlängerung im ersten Monat begründen. DSGVO Art. 12(3) · DSGVO Art. 12(6) · DSGVO Art. 15	Datenschutzbetrieb	Identitätsprüfung, Antwort und Fristenprotokoll.
Entscheide und Kommunikation bei Datenschutzverletzungen vorbereiten. Alle Verletzungen dokumentieren, auch Entscheide gegen eine Meldung. DSGVO Art. 33(5) · DSGVO Art. 34	Vorfälleleitung und Datenschutz	Verletzungsregister, Risikobewertung und Empfangsnachweise.

Empfohlene Tests und Rechtsbezug

- Einen Beschäftigten- oder Kundendatensatz von Erhebung bis Löschung verfolgen, auch bei Lieferanten.
- Auskunftsanfrage und Datenschutzvorfall simulieren; Verfügbarkeit und Vertraulichkeit berücksichtigen.

Tests dienen: [DSGVO Art. 5\(2\)](#) · [DSGVO Art. 12\(3\)](#) · [DSGVO Art. 32\(1\)\(d\)](#)

Beachten: Einwilligung ist nicht für jede Tätigkeit die Standardgrundlage. Auch verschlüsselte Daten können personenbezogen sein. Eine Datenschutzverletzung ist ohne bestätigten Datenabfluss möglich.

Rechtsgrundlagen [DSGVO Art. 5 bis 6, 12, 28, 30 bis 35](#)

DORA Praxischeckliste

DORA gilt seit 17. Januar 2025 für aufgeführte Finanzunternehmen, unter Beachtung von Ausnahmen und Verhältnismässigkeit. Normale IKT-Lieferanten unterliegen Kundenverträgen; benannte kritische IKT-Drittdienstleister einem eigenen Überwachungsrahmen.

Aus dem Gesetz „definiert, genehmigt, überwacht und verantwortet die Umsetzung“ [DORA Art. 5\(2\)](#)
 Leitungsentscheide und Nachverfolgung zum IKT-Rahmenwerk dokumentieren.

Massnahmen und Nachweise

Massnahme	Zuständigkeit empfohlen	Aufzubewahrende Nachweise
Kritische oder wichtige Funktionen mit Systemen, Daten, Personen und Lieferanten verknüpfen. Konzentration und einzelne Ausfallpunkte erkennen. DORA Art. 8(1) · DORA Art. 8(5) · DORA Art. 29(1)	Fachbereich und IT	Funktionsübersicht und Abhängigkeitsbewertung.
Genehmigten IKT-Risikorahmen sowie Kontinuitäts-, Wiederherstellungs- und Kommunikationsvorkehrungen pflegen. DORA Art. 5(2) · DORA Art. 6(1) · DORA Art. 11 · DORA Art. 14	Leitung und Risiko-management	Genehmigter Rahmen, Überprüfungen und Risikobehandlung.
Vorfälle nach geltenden Kriterien einstufen und Meldungen schwerwiegender Vorfälle vorbereiten. Kenntnisnahme und Einstufung getrennt erfassen. DORA Art. 18(1) · DORA Art. 19(1) · 2025/301 Art. 5	Vorfalleitung	Einstufungsscheckliste und Meldechronologie.
Verhältnismässiges Resilienztestprogramm betreiben. Anwendbarkeit fortgeschrittener bedrohungsorientierter Penetrationstests prüfen. DORA Art. 24(1)-(2) · DORA Art. 26	CISO und Risiko-management	Testplan, Befunde, Nachtests und TLPT-Entscheid.
Vorgeschriebenes Register der IKT-Vertragsvereinbarungen führen. Sorgfalt, Konzentration, Untervergabe und Pflichtklauseln berücksichtigen. DORA Art. 28(3)-(4) · DORA Art. 29 · DORA Art. 30	Einkauf und Recht	Register, Verträge und Anbieterbewertungen.
Kontinuität und Ausstieg bei wichtigen Abhängigkeiten testen. Nutzbare Exporte, Ersatzkompetenzen, Kapazität und realistische Zeiten bestätigen. DORA Art. 11(6) · DORA Art. 28(8)	Dienst-verantwortliche	Wiederherstellungs- oder Ausstiegsübung mit Fachabnahme.

Empfohlene Tests und Rechtsbezug

- Ausfall des Identitätsdienstes simulieren, den Produktion und Notfallwiederherstellung gemeinsam nutzen.
- Meldung eines schwerwiegenden Vorfalls innerhalb der Vier- und 24-Stunden-Grenzen auf Seite 18 vorbereiten.

Tests dienen: [DORA Art. 11\(6\)](#) · [DORA Art. 24\(1\)](#) · [2025/301 Art. 5](#)

Beachten: Auslagerung von Meldungen oder Betrieb überträgt nicht die Verantwortung des Finanzunternehmens. Eine einfache Lieferantenliste ersetzt das vorgeschriebene Informationsregister nicht.

Rechtsgrundlagen [DORA Art. 5 bis 16, 19, 24 bis 30](#) | [Meldefristen](#)

KI-Verordnung Praxischeckliste

System und Verwendungszweck einstufen. Anbieter-, Betreiber-, Einführer- oder Händlerrolle festhalten; Anwendung vom KI-Modell mit allgemeinem Verwendungszweck (GPAI) unterscheiden. Bei Änderungen neu prüfen.

Aus dem Gesetz „die Entwicklung der KI-Kompetenz“ [KI-VO geändert Art. 4\(1\)](#)

Dies ist der geänderte Artikel 4 Absatz 1; Kompetenzmassnahmen auf Nutzung und Risiken abstimmen.

Massnahmen und Nachweise

Massnahme	Zuständigkeit empfohlen	Aufzubewahrende Nachweise
KI-Nutzungen, Zuständige, Ein-/Ausgaben, Betroffene, verbundene Tools und Lieferanten inventarisieren. Vor Einsatz auf verbotene Praktiken prüfen. KI-VO Art. 2(1) · KI-VO Art. 3(3)-(4) · KI-VO Art. 5 · KI-VO geändert Art. 5(1a)	Fachbereich und Recht	KI-Register, Zweck und Verbotsprüfung.
Hochrisiko-, Transparenz- und GPAI-Pflichten prüfen. Rolle, Rechtsgrund und Geltungsbeginn festhalten; Änderungen/Umbenennung prüfen. KI-VO Art. 6 · KI-VO Art. 25(1) · KI-VO Art. 50 · KI-VO Art. 53 · 2026/1744 Art. 1(40)	KI-Governance	Freigegebene Einstufung und Änderungsanlässe.
Informations- und Kompetenzpflichten umsetzen. Nach Nutzung und Risiko schulen; erforderliche Interaktions- und Inhaltshinweise geben. KI-VO geändert Art. 4(1) · KI-VO Art. 50(1)-(4)	Fachbereich und HR	Hinweise, Schulungsunterlagen und Teilnahme.
Bei relevanten Hochrisikopflichten Anbieterdokumentation, Qualität und Konformität oder Betreiberaufsicht und Überwachung planen. KI-VO Art. 16 · KI-VO Art. 17 · KI-VO Art. 26 · KI-VO Art. 43 · 2026/1744 Art. 1(40)	Produkt oder Fachbereich	Rollenbezogene Anforderungen und Nachweisliste.
Personenbezogene Daten und schädliche Folgen bewerten. Repräsentative Fälle, Grenzen und wirksamen menschlichen Eingriff testen. DSGVO Art. 35(1) · KI-VO Art. 9 · KI-VO Art. 14 · KI-VO Art. 27(1)	Datenschutz und Fachbereich	Erforderliche DSFA, Tests und Freigabeentscheid.
Bei Agenten Tool-Rechte und Datenzugriff beschränken; Handlungsgrenzen, Freigaben und getesteten Abschaltweg vorsehen. Dient: KI-VO Art. 14(4)(d)-(e) · KI-VO Art. 15(5) · DSGVO Art. 32(1)	Entwicklung und CISO	Berechtigungsübersicht, Aktionslogs und Abschalttest.

Empfohlene Tests und Rechtsbezug

- Verantwortliche erläutern Zweck, Rechtsrolle und Zulässigkeit des Systems.
- Eine falsche Ausgabe und eine unzulässige Tool-Anweisung testen; Eingriff und Wiederherstellung prüfen.

Tests dienen: [KI-VO Art. 14](#) · [KI-VO Art. 15](#) · [2026/1744 Art. 1\(40\)](#)

Beachten: Die Agentenkontrollen der letzten Zeile sind Empfehlungen, keine vorgeschriebene Architektur. Die Änderung 2026 verschiebt Hochrisikotermine; siehe Seite 24. Andere anwendbare Pflichten bestehen fort.

Rechtsgrundlagen [KI-VO](#) | [Änderung 2026](#)

Cyber Resilience Act Praxischeckliste

Prüfen, ob das Produkt mit digitalen Elementen erfasst ist und welche Wirtschaftsakteursrolle gilt. Meldungen nach Artikel 14 gelten seit 11. September 2026; die meisten Anforderungen ab 11. Dezember 2027.

Aus dem Gesetz „mit einer sicheren Standardkonfiguration auf dem Markt bereitgestellt werden“ [CRA Anhang I Teil I \(2\) \(b\)](#)

Risikobezug, Anwendbarkeit und Ausnahme für massgeschneiderte B2B-Produkte in der vollständigen Vorschrift beachten.

Massnahmen und Nachweise

Massnahme	Zuständigkeit empfohlen	Aufzubewahrende Nachweise
Produktgrenzen, notwendige Fernverarbeitung, Versionen, EU-Inverkehrbringen und Ausnahmen festlegen. Konformitätsverfahren bestimmen. CRA Art. 2 · CRA Art. 3(1)-(2) · CRA Art. 32	Produkt und Recht	Geltungsbereich, Rolle und Konformitätsentscheid.
Cybersicherheitsrisiken des Produkts bewerten. Sicherheitsanforderungen in Design, Voreinstellungen, Zugriff und Updates integrieren. CRA Art. 13(1)-(3) · CRA Anhang I Teil I	Entwicklung	Bedrohungsbewertung, Anforderungen und Sicherheitstests.
Softwarekomponenten und Schwachstellen verfolgen. Maschinenlesbare Softwarestückliste und Offenlegungskanal vorbereiten. CRA Anhang I Teil II (1), (5)-(6)	Produkt-sicherheit	Komponenteninventar, SBOM und Eingangsmeldungen.
Lebenszyklussupport und sichere Updates finanzieren. Begründeten Supportzeitraum festlegen: grundsätzlich mindestens fünf Jahre, ausser die erwartete Nutzung ist kürzer. CRA Art. 13(8) · CRA Art. 13(19) · CRA Anhang I Teil II (7)-(8)	Produkt-management	Supportentscheid, veröffentlichtes Enddatum und Updatetests.
Technische Unterlagen, Pflichtanleitungen, EU-Erklärung und CE-Kennzeichnung im einschlägigen Konformitätsverfahren erstellen. CRA Art. 13(12) · CRA Art. 28 · CRA Art. 30 · CRA Art. 31 · CRA Art. 32	Produkt und Qualität	Freigabeakte und Konformitätsnachweise.
Meldungen für relevante ausgenutzte Schwachstellen und schwerwiegende Vorfälle bereits betreiben. Erfasste Altprodukte nach Artikel 69 einbeziehen. CRA Art. 14(1)-(4) · CRA Art. 69(3) · CRA Art. 71	Produkt-reaktionsteam	24-Stunden-Kontaktweg, Einstufung und Meldungen.

Empfohlene Tests und Rechtsbezug

- Bei einem freigegebenen Produkt betroffene Versionen, Komponenten, Supportverantwortliche und Kundenkontakt bestimmen.
- Schwachstellenszenario von Bewertung und Meldung bis zur Korrekturverteilung und Nutzeranleitung durchspielen.

Tests dienen: [CRA Art. 13\(2\)](#) · [CRA Art. 14](#) · [CRA Anhang I Teil II](#)

Beachten: Eigenständiges SaaS ist nicht automatisch ein CRA-Produkt. Notwendige Fernverarbeitung kann Produktbestandteil sein. Support muss die erwartete Nutzung berücksichtigen; fünf Jahre reichen nicht immer.

Rechtsgrundlagen [CRA Art. 13, 14, 32, 69 und 71](#)

Resilienz kritischer Einrichtungen Praxischeckliste

CER betrifft die Resilienz benannter kritischer Einrichtungen und wesentlicher Dienste gegen physische und andere Störungen. Nationale Einstufung und Mitteilung prüfen. Sektorale Ausnahmen beachten, etwa für Banken, Finanzmarktinфраstruktur und digitale Infrastruktur.

Aus dem Gesetz „geeignete und verhältnismässige technische, sicherheitsbezogene und organisatorische Massnahmen zur Gewährleistung ihrer Resilienz“ [CER Art. 13\(1\)](#)

Massnahmen mit Risikobewertung und nationaler Umsetzung verknüpfen.

Massnahmen und Nachweise

Massnahme	Zuständigkeit empfohlen	Aufzubewahrende Nachweise
Mitteilung, Eingangsdatum, Dienst, Behörde und Pflichten erfassen. Sektorale und nationale Ausnahmen prüfen. CER Art. 6(3) · CER Art. 8	Recht und Kontinuität	Einstufungsakte und geltende Fristen.
Natürliche und menschlich verursachte Gefahren bewerten: Strom, Wasser, Zugang, Personal, Sabotage und grenzüberschreitende Abhängigkeiten. CER Art. 12(1)-(2)	Kontinuität und Infrastruktur	Gefahrenübergreifende Risikobewertung.
Standorte und Betrieb angemessen schützen. Zugang, physische Sicherungen und zulässige Personalmassnahmen festlegen. CER Art. 13(1)(a)-(b), (e) · CER Art. 14	Infrastruktur und HR	Kontrollen, genehmigte Zugänge und rechtmässige Prüfungen.
Kontinuität, Ersatzabläufe und Wiederherstellung planen. Ressourcen, Alternativen und tragfähige Mindestleistungen klären. CER Art. 13(1)(c)-(d)	Fachverantwortliche	Resilienzplan und Vereinbarungen zu Abhängigkeiten.
Personal schulen und Störungen üben. Kontaktperson benennen und erhebliche Vorfallmeldungen vorbereiten. CER Art. 13(1)(f) · CER Art. 13(3) · CER Art. 15(1)	Kontinuitätsleitung	Übung, Kontaktkarte und Meldeprozess.
Fristen ab Mitteilung verfolgen. Risikobewertung innerhalb von neun Monaten; Kapitel III grundsätzlich nach zehn Monaten. CER Art. 6(3) · CER Art. 12(1)	Recht und Sponsor	Datierter Plan mit Bezug auf die tatsächliche Mitteilung.

Empfohlene Tests und Rechtsbezug

- Langen Strom- oder Wasserausfall mit gesperrtem Standort und Ausfall eines Schlüssellieferanten üben.
- Zeigen, welcher Mindestdienst wie lange mit welchen Personen und Ressourcen weiterläuft.

Tests dienen: [CER Art. 13\(1\)\(c\)-\(d\), \(f\)](#)

Beachten: Ein Cyber-Wiederherstellungsplan allein deckt physische Resilienz nicht ab. NIS2-/CER-Einstufung und lokale Pflichten separat erfassen, auch bei gemeinsamen Nachweisen.

Rechtsgrundlagen [CER Art. 6, 8 und 12 bis 15](#)

Data Act Praxiseckliste

Rollen zuordnen: Hersteller vernetzter Produkte, Anbieter verbundener Dienste, Nutzer, Dateninhaber, Datenempfänger oder Datenverarbeitungsanbieter. Cloud-Kunden sollten Wechselrechte auch in Einkauf und Ausstiegsplanung nutzen.

Aus dem Gesetz „Anbieter von Datenverarbeitungsdiensten treffen die in den Artikeln 25, 26, 27, 29 und 30 vorgesehenen Maßnahmen“ [Data Act Art. 23](#)

Vollständige Wechselflicht einschliesslich Rolle, Umfang und Ausnahmen lesen.

Massnahmen und Nachweise

Massnahme	Zuständigkeit empfohlen	Aufzubewahrende Nachweise
Produkt- und Dienstdaten, Metadaten, Zugangswege und Inhaber jedes Datensatzes bestimmen. Data Act Art. 2(15)-(17) · Data Act Art. 3(1)	Produkt- und Datenverantwortliche	Datenkatalog und Rollenübersicht.
Pflichtinformationen vor Vertrag und erforderlichen Nutzerzugang bereitstellen. Identität und Befugnis ohne hinderliche Verfahren prüfen. Data Act Art. 3(2)-(3) · Data Act Art. 4(1)	Produkt und Betrieb	Informationen, Anfrageweg und gelieferte Datenprobe.
Zulässige Weitergabe an Dritte bearbeiten. DSGVO, Geschäftsgeheimnisse, Nutzungszwecke und Schutzmassnahmen prüfen. Data Act Art. 4(6)-(9) · Data Act Art. 5 · Data Act Art. 6	Recht und Datenschutz	Weitergabeentscheid, Schutzmassnahmen und Zugangsbedingungen.
Datenklauseln auf Missbräuchlichkeit und Transparenz prüfen. Verbindliche Behördenanfragen durch Recht bewerten lassen. Data Act Art. 13 · Data Act Art. 14 · Data Act Art. 17	Recht und Einkauf	Vertragsprüfung und Anfragebewertung.
Für erfasste Cloud-/Verarbeitungsdienste exportierbare Daten, Schnittstellen, Übergang, Unterstützung, Entgelte und Löschung definieren. Data Act Art. 25 · Data Act Art. 27 · Data Act Art. 29 · Data Act Art. 30	Dienstverantwortliche	Vertrag und umsetzbarer Wechselplan.
Export in eine alternative Umgebung testen; Datensätze abgleichen und Funktions- oder Interoperabilitätsgrenzen erfassen. Dienst: Data Act Art. 23(c)-(d) · Data Act Art. 30	IT und Fachbereich	Export-/Importtest und Ausstiegsmassnahmen.

Empfohlene Tests und Rechtsbezug

- Repräsentative Daten eines vernetzten Produkts anfordern; Vollständigkeit, Format, Metadaten und Berechtigung prüfen.
- Exportierte Cloud-Daten mit unabhängigem Tool lesen; tatsächliche Dauer und Aufwand messen.

Tests dienen: [Data Act Art. 4\(1\)](#) · [Data Act Art. 23\(c\)](#) · [Data Act Art. 30](#)

Beachten: Der Data Act gewährt keinen generellen Zugang zu allen Unternehmensdaten und verdrängt die DSGVO nicht. Der Wegfall von Wechselentgelten beseitigt nicht jede Dienstgebühr oder Vorfälligkeitszahlung.

Rechtsgrundlagen [Data Act Art. 3 bis 5, 13, 23 bis 31 und 50](#)

eIDAS und digitales Vertrauen Praxischeckliste

Nutzende Unternehmen von Anbietern regulierter Vertrauensdienste unterscheiden. Die Checkliste beginnt beim vertrauenden Unternehmen; Anbieter und Wallet-Beteiligte benötigen zusätzliche rollenbezogene Anforderungen.

Aus dem Gesetz „Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift.“ [eIDAS Art. 25\(2\)](#)

Zeichnungsbefugnis und nationale Formvorgaben separat prüfen.

Massnahmen und Nachweise

Massnahme	Zuständigkeit empfohlen	Aufzubewahrende Nachweise
Transaktionen, Länder, Parteien und Formvorgaben erfassen. Je Prozess benötigtes Signatur- oder Siegelniveau festlegen. Dienst: eIDAS Art. 2(3) · eIDAS Art. 25 · eIDAS Art. 35	Recht und Prozessverantwortliche	Zuordnung von Transaktionen zu Signaturniveaus.
Dienst auswählen und prüfen. Bei erforderlichem qualifiziertem Status den konkreten Dienst in den amtlichen Vertrauenslisten kontrollieren. eIDAS Art. 22(1) · eIDAS Art. 32(1)	Einkauf und Recht	Datierter Nachweis des Dienstestatus.
Identität und Zeichnungsbefugnis prüfen. Signaturzugänge schützen; Delegation, Widerruf und Austritte regeln. Dienst: eIDAS Art. 26 · eIDAS Art. 32(1)	Identität und Fachbereich	Identitätsnachweis und Zeichnungsbefugnis.
Signierte Datei, Validierung, Zertifikate, Zeitangaben und Nachweise für spätere Prüfung erhalten. Dienst: eIDAS Art. 32(1) · eIDAS Art. 34	Aktenverantwortliche	Validierungs- und Aufbewahrungsunterlagen.
Validierung ausserhalb des Anbieterportals testen. Langzeitzugang für Vertragsende oder Anbieterausfall sichern. Dienst: eIDAS Art. 32 · eIDAS Art. 34	IT und Aktenführung	Unabhängige Validierung und Exporttest.
Bei Identitäts- oder Vertrauensdiensten Konformität, Aufsicht, Vorfälle und EUDI-Wallet-Pflichten separat bewerten. eIDAS Art. 5a · eIDAS Art. 19a · eIDAS Art. 20 · eIDAS Art. 24	Dienstverantwortliche und Recht	Rollenbezogener Compliance- und Meldeplan.

Empfohlene Tests und Rechtsbezug

- Signiertes Dokument prüfen, ohne nur auf Screenshot oder Freigabemail des Anbieters zu vertrauen.
- Prüfen, ob die unterzeichnende Person zum Signaturzeitpunkt zur Transaktion befugt war.

Tests dienen: [eIDAS Art. 32](#) · [eIDAS Art. 34](#)

Beachten: Eine qualifizierte elektronische Signatur wirkt in der EU wie eine handschriftliche Unterschrift, belegt aber allein keine Unternehmensvollmacht und erfüllt nicht jede nationale Formvorgabe. Ein elektronisches Siegel ist ein anderes Instrument.

Rechtsgrundlagen [eIDAS Art. 22, 25, 32 und 35](#) | [EU-Vertrauenslisten](#)

Digital Services Act Praxischeckliste

Dienste einstufen: reine Durchleitung, Caching, Hosting, Plattform, Verbrauchermarktplatz oder benannter sehr grosser Dienst. Eine Firmenwebsite mit eigenen Inhalten ist nicht automatisch eine DSA-Plattform.

Aus dem Gesetz „Diese Verfahren müssen leicht zugänglich und benutzerfreundlich sein“ [DSA Art. 16\(1\)](#)

Hosting-Meldeverfahren mit einer realistischen Nutzermeldung testen.

Massnahmen und Nachweise

Massnahme	Zuständigkeit empfohlen	Aufzubewahrende Nachweise
Funktionen, EU-Nutzer und Betreiber dokumentieren. Genaue Reichweite grössenbezogener Ausnahmen prüfen. DSA Art. 2(1) · DSA Art. 3(g), (i) · DSA Art. 19(1) · DSA Art. 29	Produkt und Recht	Diensteinstufung und Ausnahmeprüfung.
Erforderliche Kontakte und Bedingungen veröffentlichen. Inhaltsbeschränkungen und Moderationsregeln verständlich erklären. DSA Art. 11(1) · DSA Art. 12(1) · DSA Art. 14(1)	Recht und Betrieb	Kontaktstellen, Bedingungen und Veröffentlichungsnachweis.
Für Hosting nutzbare Meldungen rechtswidriger Inhalte einrichten. Fälle sorgfältig prüfen, Entscheide erfassen und vorgeschriebene Begründungen mitteilen. DSA Art. 16(1)-(6) · DSA Art. 17(1)-(3)	Vertrauen und Sicherheit	Meldung, Bewertung, Entscheid und Kommunikation.
Bei erfassten Plattformen Beschwerden bearbeiten sowie Werbe-, Oberflächen- und Minderjährigenschutzpflichten prüfen. DSA Art. 20(1) · DSA Art. 25 · DSA Art. 26 · DSA Art. 28	Produkt und Betrieb	Beschwerdeergebnisse und Designprüfungen.
Bei erfassten Verbrauchermarktplätzen Händlernachverfolgbarkeit und anwendbare Konformität durch Gestaltung umsetzen. DSA Art. 30(1)-(3) · DSA Art. 31	Marktplatz-verantwortliche	Händlerprüfungen und Tests der Angebotsabläufe.
Nutzerzahlen und Benennung verfolgen. Bei Einstufung als sehr gross das zusätzliche Systemrisiko- und Prüfregime umsetzen. DSA Art. 24(2) · DSA Art. 33 · DSA Art. 34 · DSA Art. 37	Compliance	Nutzerberechnung, Benennung und Prüfplan.

Empfohlene Tests und Rechtsbezug

- Realistische Meldung rechtswidriger Inhalte bis zum begründeten Entscheid verfolgen.
- Nutzerbeschwerde testen und prüfen, ob der Betrieb einen früheren Fehler korrigieren kann.

Tests dienen: [DSA Art. 16\(6\)](#) · [DSA Art. 20\(4\)](#)

Beachten: Ausnahmen für Kleinst- und Kleinunternehmen betreffen einzelne Pflichten, nicht den ganzen Rechtsakt. Artikel 18 betrifft bestimmte Verdachtsfälle von Straftaten gegen Leben oder Sicherheit; es gibt keine allgemeine 72-Stunden-Cybermeldefrist im DSA.

Rechtsgrundlagen [DSA Art. 11 bis 18, 19 bis 32 und 33 bis 42](#)

Die erste Stunde eines Vorfalls steuern

Eindämmung und rechtliche Einordnung gleichzeitig starten. Die Zeiten sind interne Empfehlungen, keine gesetzlichen Meldefristen. Eine Pflichtmeldung nicht bis zur Ursachenbestätigung aufschieben.

Ziel	Massnahme	Ergebnis
0 bis 15 Minuten	Vorfalleitung und Protokollführung benennen. Sicherheit schützen, Kontaktweg aktivieren und Logs sichern. Entdeckung und bekannte Ereigniszeiten in UTC erfassen. Dient: NIS2 Art. 21(2)(b) · DORA Art. 17(3)(a)	Fall-ID, Chronologie und erster Betroffenheitsumfang.
15 bis 30 Minuten	Nach genehmigten Verfahren eindämmen. Bei OT vor störenden Eingriffen möglichst Sicherheits- oder Werksverantwortliche einbinden. Betroffene Einrichtungen, Dienste, Produkte und Daten bestimmen. Dient: DORA Art. 17(3)(b), (f) · NIS2 Art. 21(2)(b)	Eindämmungsentscheide und Geschäftsauswirkung.
Bis 30 Minuten	Recht, Datenschutz, Fach- und Produktverantwortliche beiziehen. Jeden Meldetatbestand prüfen und Zeitpunkte der rechtlichen Kenntnisnahme oder Einstufung erfassen. Dient: DSGVO Art. 33(1) · NIS2 Art. 23(3) · DORA Art. 18(1)	Getrennte Meldeentscheide und Fristen.
Bis 60 Minuten	Je Meldeweg Absender und Stellvertretung benennen. Fakten, Unbekanntes und Schutzmassnahmen entwerfen. Kunden- und Vertragsmeldungen klären. Dient: DSGVO Art. 33(3)-(4) · NIS2 Art. 23(4) · DORA Art. 19(1)	Freigegebene Erstmeldungen oder dokumentierter Nichtmeldeentscheid.

Eine Chronologie und getrennte Rechtsfristen führen

Erkennung, rechtliche Kenntnisnahme je Regelwerk, Einstufung als schwerwiegend/erheblich, Entscheide, Meldungen und Bestätigungen erfassen. Ein Ereignis kann mehrere Gesetze für verschiedene Konzerneinheiten auslösen. Eine Meldung erfüllt nicht automatisch alle Regime.

Mindestinhalt der Vorfälle

- Fall-ID; Rechtsträger; Leitung und Stellvertretung; betroffene Dienste, Länder, Daten und Produktversionen.
- Bestätigte Fakten; Hypothesen; Folgen für Betrieb und Personen; Quellen und Zeitstempel jeder Aktualisierung.
- Meldetatbestand je Gesetz; genaue Frist; Empfänger; Freigabe; Absender; Empfang; nächste Aktualisierung.
- Eindämmung, Wiederherstellung, Nachweisablage und Kundenschutz.

Vor dem Abschluss

Vollständigkeit aller Aktualisierungen und Abschlussberichte bestätigen. Ursache, Dienst-/Datenwiederherstellung, Restrisiko, Massnahmen, Zuständige und Nachtests erfassen. Nichtmeldeentscheide begründen und bei neuen Fakten überprüfen.

Rechtsgrundlagen [DSGVO Art. 33 und 34](#) | [NIS2 Art. 23](#) | [DORA-Melderegeln](#)

Zentrale Meldefristen für Vorfälle

EU-Regeln mit nationalem Meldeweg, Schwellenwerten, zuständiger Behörde und technischen Standards anwenden. Alle Fristen sind Höchstgrenzen; die Pflicht zum unverzüglichen Handeln bleibt bestehen.

Regelwerk und Auslöser	Erste Meldung	Folgemeldung und Empfänger
DSGVO Verantwortlicher Datenschutzverletzung, ausser ein Risiko für Rechte und Freiheiten ist unwahrscheinlich.	Unverzüglich, möglichst innerhalb von 72 Stunden nach Bekanntwerden. Verzögerung begründen.	Zuständige Datenschutzbehörde. Fehlende Angaben schrittweise ohne unangemessene weitere Verzögerung nachreichen. Alle Verletzungen dokumentieren. DSGVO Art. 33(1), (3)-(5)
DSGVO Auftragsverarbeiter und Betroffene	Auftragsverarbeiter: Verantwortlichen unverzüglich informieren. Verantwortlicher: Betroffene bei hohem Risiko unverzüglich benachrichtigen, vorbehaltlich Artikel 34.	Für Auftragsverarbeiter keine pauschalen 72 Stunden annehmen. Vertragsfristen separat verfolgen. DSGVO Art. 33(2) · DSGVO Art. 34(1)-(3)
NIS2 Erheblicher Sicherheitsvorfall nach geltenden Kriterien.	Frühwarnung innerhalb von 24 Stunden ab Kenntnis eines erheblichen Vorfalls; Vorfallmeldung innerhalb von 72 Stunden. Beides unverzüglich.	Zuständiges CSIRT oder Behörde. Abschlussbericht binnen eines Monats nach Vorfallmeldung; Zwischenbericht auf Verlangen. NIS2 Art. 23(3) · NIS2 Art. 23(4)(a)-(d)
NIS2 laufender Vorfall und Vertrauensdienste	Vertrauensdiensteanbieter: Für einschlägige Vorfälle gilt eine Vorfallmeldefrist von 24 statt 72 Stunden.	Bei fortdauerndem Vorfall zunächst Fortschrittsbericht, dann Abschlussbericht binnen eines Monats nach Bewältigung. NIS2 Art. 23(4)(b), (e)
DORA Schwerwiegender IKT-Vorfall nach geltenden Einstufungsregeln.	So früh wie möglich: binnen vier Stunden nach Einstufung als schwerwiegend, spätestens 24 Stunden nach Kenntnis. Bei Einstufung nach 24 Stunden: binnen vier Stunden ab Einstufung.	Zuständige Finanzbehörde. Zwischenbericht binnen 72 Stunden nach Erstmeldung; Aktualisierung bei Wiederherstellung. Abschluss binnen eines Monats nach Zwischenbericht oder letzter aktualisierter Zwischenmeldung. DORA Art. 19(1) · 2025/301 Art. 5(1)-(4)

Fristen vor der Übung einrichten

Je Einrichtung Portal, Behörde, Schwellenwerte, lokale Formulare, Absender und Stellvertretung auf Seite 22 eintragen. Zugang ohne echte Vorfallmeldung testen.

DORA enthält Sonderregeln und Ausnahmen für Wochenenden und Feiertage. Durchgehende Erreichbarkeit als Betriebsstandard vorsehen; Verlängerungen nur nach Prüfung der Voraussetzungen von Artikel 5 und möglicher Behördenentscheide nutzen.

Rechtsgrundlagen [DSGVO Art. 33 und 34](#) | [NIS2 Art. 23](#) | [DORA Verordnung 2025/301 Art. 5](#)

Produktbezogene und weitere Meldewege

Diese Wege ergänzen, wenn Tätigkeit und Rechtsrolle sie erfordern. Geltungsbeginn und nationale Umsetzung prüfen; keine einheitliche Pauschalfrist anwenden.

Regelwerk und Auslöser	Frist und praktischer Meldeweg
CRA Aktiv ausgenutzte Schwachstelle	Hersteller meldet über die zentrale Plattform an koordinierendes CSIRT und ENISA. Frühwarnung binnen 24 Stunden ab Kenntnis; Schwachstellenmeldung binnen 72 Stunden. Abschlussbericht binnen 14 Tagen nach Verfügbarkeit einer Korrektur- oder Abhilfemassnahme. CRA Art. 14(1)-(2)
CRA Schwerwiegender Vorfall mit Auswirkung auf Produkt- sicherheit	Gleiche Empfänger und Plattform. Frühwarnung binnen 24 Stunden ab Kenntnis; Vorfallmeldung binnen 72 Stunden. Abschlussbericht binnen eines Monats nach Vorfallmeldung. Nutzerinformation nach Artikel 14 beachten. CRA Art. 14(3)-(4), (8)
CER Erhebliche oder potenziell erhebliche Störung wesentlicher Dienste	Zuständige Behörde unverzüglich informieren; Erstmeldung binnen 24 Stunden ab Kenntnis, ausser betrieblich nicht möglich. Gegebenenfalls Detailbericht binnen eines Monats; nationale Regel im lokalen Ablaufplan umsetzen. CER Art. 15(1)
KI-VO Schwerwiegender Vorfall mit Hochrisiko-KI	Zuerst Rolle und Übergangsregeln prüfen. Anbieter meldet sofort bei Kausalzusammenhang oder begründeter Wahrscheinlichkeit, spätestens binnen 15 Tagen ab Kenntnis. Weitverbreiteter Verstoss oder kritische Infrastruktur nach Art. 3(49)(b): sofort, binnen zwei Tagen. Todesfall: sofort bei vermutetem Zusammenhang, binnen zehn Tagen. An zuständige Marktaufsicht oder KI-Büro nach geändertem Art. 75. KI-VO Art. 73(1)-(4) · KI-VO Art. 26(5) · KI-VO geändert Art. 75(1a)
eIDAS Sicherheitsverletzung oder Störung eines Vertrauensdienstes	Nicht qualifizierte Anbieter: Art. 19a verlangt unverzüglich und binnen 24 Stunden ab Kenntnis. Qualifizierte Anbieter: Art. 24(2)(fb) verlangt unverzüglich und binnen 24 Stunden nach dem Vorfall. Aufsicht und weitere vorgeschriebene Empfänger informieren. NIS2/DSGVO separat prüfen; dies sind Anbieterpflichten. eIDAS Art. 19a(1)(b) · eIDAS Art. 24(2)(fb)
DSA Verdacht auf bestimmte Straftaten	Hosting-Anbieter müssen bei gesetzlichem Auslöser bezüglich Leben oder Sicherheit unverzüglich die zuständige Strafverfolgungs- oder Justizbehörde nach Artikel 18 informieren. Dies ist von Cybervorfallmeldungen getrennt. DSA Art. 18(1)-(2)

Betriebsregel: Produktversionen, Supportstatus, Betroffene, Schutzschritte und weiterhin sensible Informationen erfassen. Recht und Produktverantwortliche stimmen Behörden- und Kundenkommunikation ab. Vertrags-, Versicherungs- und weitere Sektormeldungen in derselben Chronologie führen.

Rechtsgrundlagen [CRA Art. 14](#) | [CER Art. 15](#) | [KI-VO Art. 73](#) | [KI-Änderung](#) | [eIDAS](#) | [DSA Art. 18](#)

Eine gemeinsame Lieferantenprüfung nutzen

Bei Auswahl, Verlängerung und wesentlicher Änderung prüfen. Aufwand nach Dienstwirkung, Daten, Zugang und Rechtsrolle bemessen, nicht nur nach Kosten. Kleine Lieferanten mit privilegiertem Zugang zu kritischen Systemen besonders prüfen.

Entscheidung	Frage an Lieferant oder Verantwortliche	Anzufordernde Nachweise
Umfang und Wirkung	Welcher Rechtsträger liefert den Dienst? Welche Funktionen, Daten und Systeme hängen davon ab? Dient: DORA Art. 28(3)-(4) · DSGVO Art. 28(1)	Dienstbeschreibung, Standorte und Abhängigkeitsübersicht.
Zugriff und Daten	Wer administriert? Welche Unterauftragsverarbeiter oder Standorte verarbeiten Daten? Wie werden Zugriff und Löschung gesteuert? Dient: DSGVO Art. 28(2)-(3) · DSGVO Art. 44	Zugriffsmodell, Verarbeitungsklauseln und Datenflussangaben.
Sicherheit und Resilienz	Was wird getestet? Welche Ausnahmen bleiben? Kann der Lieferant unsere Wiederanlaufanforderungen erfüllen? Dient: NIS2 Art. 21(2)(d) · DORA Art. 28(4)(c)-(d)	Relevanter Prüfbericht, offene Befunde und Wiederherstellungsnachweise.
Zusammenarbeit bei Vorfällen	Wie schnell, von wem und mit welchen Fakten werden wir informiert? Ist Hilfe ausserhalb der Bürozeiten verfügbar? Dient: DSGVO Art. 28(3)(f) · DORA Art. 30(2)(f), (3)(b)	Vereinbarte Meldepflichten und getesteter Kontaktweg.
Prüfung und Änderungen	Erhalten wir Nachweise? Welche Änderungen, Untervergaben oder Dienstunterbrechungen müssen gemeldet werden? Dient: DSGVO Art. 28(3)(h) · DORA Art. 30(2)(a), (3)	Verträge, Änderungsrechte und Zuständigkeitsmatrix.
Ausstieg und Portabilität	Können wir nutzbare Daten exportieren, den Dienst wechseln und Löschung bestätigen? Welche Zeit, Kosten und Abhängigkeiten bleiben? Dient: DORA Art. 28(8) · Data Act Art. 25(2)	Ausstiegsplan, Probeexport und Kündigungsbedingungen.
Gesetzesspezifische Klauseln	Liegt DSGVO-Verarbeitung vor? Gilt DORA für den Kunden? Sind Data Act, KI- oder Produktpflichten relevant? Dient: DSGVO Art. 28(3) · DORA Art. 30(2)-(3) · Data Act Art. 25	Ausgefüllte Checkliste der anwendbaren Rechtsvorgaben.

Expliziten Freigabeentscheid treffen

Genehmigen, mit befristeten Auflagen genehmigen oder ablehnen/pausieren. Lücken, Ersatzmassnahmen, Fachverantwortung und Prüftermin beifügen. Nicht erfüllbare Pflichtklauseln oder Rechtspflichten eskalieren.

Abnahmetest

Einen kritischen Lieferanten auswählen. Eskalationsweg anrufen, Prüfumfang untersuchen, repräsentative Daten exportieren und tragfähige Kontinuitäts- oder Ausstiegsoption bestimmen. Fehler als Massnahmen erfassen, statt nur den Fragebogen abzulegen.

Rechtsgrundlagen [DSGVO Art. 28](#) | [NIS2 Art. 21](#) | [DORA Art. 28 bis 30](#) | [Data Act Kapitel VI](#)

Die ersten 90 Tage umsetzen

Empfohlener Umsetzungsplan. Gesetzliche Fristen, laufende Vorfälle und kritische Exposition haben Vorrang. Überfällige Pflichten sofort angehen, nicht auf eine spätere Phase verschieben.

Wann	Arbeitspaket	Verantwortliche Leitung	Abnahmekriterien
Tag 1 bis 10	Geltungsbereich je Rechtsträger und Tätigkeit klären. Nationale Gesetze, Behörden und Meldepflichten bestimmen. Dient: NIS2 Art. 2 · DSGVO Art. 3 · DORA Art. 2	Leitungssponsor und Recht	Jede prioritäre Einrichtung hat eine geprüfte Abgrenzung oder eine terminierte offene Frage.
Tag 1 bis 15	Dringende Zugriffs- und Expositions-lücken beheben; kritische Backups und Vorfällekontakte prüfen. Dient: NIS2 Art. 21(2)(c), (i)-(j) · NIS2 Art. 23	CIO und CISO	Kritische Exposition ist behoben oder abgesichert; der Meldeweg funktioniert.
Tag 11 bis 30	Kontroll- und Gesetzesverantwortliche benennen. Nachweisindex und priorisiertes Massnahmenregister erstellen. Dient: NIS2 Art. 20(1) · DORA Art. 5(2)(c) · DSGVO Art. 24(1)	Programmleitung	Jede prioritäre Lücke hat Zuständigkeit, Frist und Abschlusstest.
Tag 16 bis 45	Kritische Lieferanten und personenbezogene Datenflüsse prüfen. KI- und Produktaktivitäten einstufen. Dient: DORA Art. 28(4) · DSGVO Art. 30 · KI-VO Art. 6 · CRA Art. 2	Fach- und Spezialverantwortliche	Verträge, Einstufungen und betriebliche Lücken sind erfasst.
Tag 31 bis 60	Prioritäre Kontrollen umsetzen; Wiederherstellung, privilegierte Zugänge und Meldungen testen. Dient: NIS2 Art. 21(2)(f) · DORA Art. 11(6)	Dienstverantwortliche	Tests liefern reale Ergebnisse; Fehler haben finanzierte Korrekturen.
Tag 61 bis 75	Korrekturen nachtesten. Nachweise stichprobenartig und Rechtsänderungen prüfen. Dient: NIS2 Art. 21(2)(f) · DORA Art. 6(5)-(6)	Prüfung und Recht	Abschlussentscheide sind belegt; die Anwendbarkeit ist aktuell.
Tag 76 bis 90	Leitung prüft Restrisiken, Ressourcen und nächstes Quartal. Dient: NIS2 Art. 20(1) · DORA Art. 5(2)(g)	Sponsor in der Geschäftsleitung	Entscheide, Budget, Meilensteine und offene Rechtsfragen sind eindeutig.

Priorisierungsregel

Priorität 1: aktuelle Rechtsverletzung, unmittelbar fällige Meldung oder kritische Betriebsexposition. Priorität 2: wesentliche Kontrolllücken mit Folgen für wichtige Dienste oder Personen. Priorität 3: Verbesserungen nach Beherrschung der ersten beiden Kategorien. Bei neuen Fakten neu einstufen.

Entscheidungen statt Aktivitätszahlen berichten

Zeigen, was ausfallen kann, welche Pflicht betroffen ist, wer korrigiert, wann getestet wird und welchen Leitungsentscheid es braucht. Viele Richtlinien oder Schulungen allein belegen keine operative Wirksamkeit.

Vorlagen für Geltungsbereich und Behörden

Felder in das bestehende Register übernehmen. Je Einrichtung und Tätigkeit einen Eintrag mit Nachweisen und Prüfentscheid erstellen. Felder in Klammern sind vom Team auszufüllen.

Empfohlene Vorlagen dienen: [NIS2 Art. 2](#) · [NIS2 Art. 23\(4\)](#) · [DSGVO Art. 33\(3\)](#)

Geltungsbereich

Feld	Ausfüllen
Datensatz und Gegenstand	[ID] [Rechtsträger] [Land] [Tätigkeit oder Produkt]
Geschäftliche und rechtliche Rolle	[Dienst und Kunden] [EU-Bezug] [Verantwortlicher/Anbieter/Betreiber/andere Rolle]
Rechtsgrundlage	[Rechtsakt] [Artikel] [Link zum nationalen Recht] [Geprüfte Fassung]
Fakten und Schlussfolgerung	[Grösse und Sektor] [Ausnahmen] [Gilt jetzt / später / nicht / ungeklärt]
Geltungsdaten	[Pflichtbeginn] [Registrierungsfrist] [Eingang der Einstufung, falls relevant]
Entscheid und Überprüfung	[Verantwortliche] [Rechtsprüfung] [Freigabedatum] [Nächste Prüfung] [Änderungsanlass]

Behörden- und Meldekarte

Feld	Je Meldeweg ausfüllen
Meldeweg und Auslöser	[Einrichtung] [Gesetz] [Quelle der Schwelle] [Fristbeginn und Dauer]
Behörde	[Behörde oder CSIRT] [Amtliche Portal-URL] [Telefonischer Ersatzweg]
Personen	[Absender und Mobilnummer] [Stellvertretung und Mobilnummer] [Freigabe und Eskalation]
Zugang und Einreichung	[Kontozuständigkeit] [Authentisierung] [Vorlagenablage] [Empfangsnachweisablage]
Test	[Letzter Zugangstest] [Ergebnis] [Offene Frage und Zuständigkeit]

Vor Freigabe des Datensatzes

- Recht hat Einrichtung, Rolle, nationale Vorschrift und Geltungsbeginn geprüft.
- Absender und Stellvertretung haben Portalzugang; Ersatzkontakte sind offline verfügbar.
- Zugangsdaten liegen im freigegebenen Tresor, nicht in dieser Vorlage.

Qualitätsprüfung: Fehlen Fakten, Status «ungeklärt» verwenden. Zuständigkeit und Frist festlegen, statt eine Ausnahme zu unterstellen.

Vorlagen für Massnahmen und Nachweise

Je Lücke eine Massnahme mit Rechtsanforderung und Kontrolle verknüpfen. Sensible Nachweise geschützt ablegen; das Register verweist darauf, statt sie zu duplizieren.

Datenfeld	Einzutragen
Anforderung und Lücke	[Massnahmen-ID] [Einrichtung] [Gesetz und Artikel] [Konkrete Lücke und Folgen]
Massnahme und Zuständigkeit	[Massnahme] [Namentlich Verantwortliche] [Umsetzungsteam] [Priorität] [Frist]
Übergangsbehandlung	[Ersatzkontrolle] [Freigabe] [Ablauf] [Rechtliche Zulässigkeit geprüft]
Abschlusstest	[Bestand und Methode] [Soll-Ergebnis] [Testdatum] [Prüfer]
Nachweis und Status	[Nachweislink] [Umfang und Zeitraum] [Ist-Ergebnis] [Offen / in Arbeit / getestet / geschlossen]

Ausgefülltes Beispiel

Lücke: Privilegierter Lieferantenzugang zu einem kritischen Dienst ohne starke Authentisierung. Massnahme: Genehmigte Authentisierung durchsetzen und ungenutzte Konten entfernen. Zuständig: Identitätsdienst. Abschluss: Jeden Zugang testen und aktive Konten abgleichen. Nachweise: Datierte Konfiguration, Tests und genehmigte Ausnahmen. Der konkreten Sicherheitsanforderung zuordnen; nicht das gesamte Gesetz als erfüllt markieren.

Empfohlene Vorlagen und Ziele dienen: [NIS2 Art. 21\(2\)\(f\)](#) · [DORA Art. 6\(5\)-\(6\)](#) · [DSGVO Art. 24\(1\)](#)

Monatliches Leitungsdashboard

Kennzahl	Empfohlenes Ziel	Eskalation, wenn
Prioritäre Einrichtungen mit freigegebenem Geltungsbereich	100 % des prioritären Umfangs	Eine regulierte Tätigkeit ungeklärt oder überfällig ist.
Überfällige Priorität-1-Massnahmen	0	Eine Massnahme überfällig bleibt.
Kritische Dienste mit bestandenen Wiederherstellungstests	100 % der geplanten Tests	Ein Dienst sein Wiederherstellungsziel verfehlt.
Kritische Zugänge erfüllen den Standard	100 % oder genehmigte befristete Behandlung	Ein exponierter Zugang nicht ausreichend geschützt ist.
Meldewege mit getestetem Zugang und Stellvertretung	100 % der anwendbaren Wege	Ein erforderlicher Weg nicht nutzbar ist.
Abgeschlossene Massnahmen mit unabhängig geprüftem Nachweis	100 % der geprüften Abschlüsse	Ein Abschluss nur auf Richtlinie oder Behauptung beruht.

Diese Ziele sind Leitungsempfehlungen, keine rechtlichen Freistellungen. Bezugsgrössen, Zeitraum und Nachweisquellen definieren. Rechtspflicht, Kontrollabdeckung und Testergebnis getrennt halten.

Termine und Rechtsänderungen verfolgen

Rechtsstand: 8. Oktober 2026. Vor wesentlichen Geltungs- oder Meldeentscheiden Rechtsänderungen und nationale Umsetzung prüfen. Verwendete Fassung und Geltungsdatum im Rechtsregister festhalten.

Rechtsakt	Datum oder Auslöser	Praktische Massnahme
NIS2	EU-Umsetzungsfrist war der 17. Oktober 2024.	Nationales Recht, Registrierung und lokale Melderegeln prüfen. NIS2 Art. 41(1)
DORA	Anwendbar seit 17. Januar 2025.	Rahmenwerk und aktuelle technische Standards jetzt betreiben. DORA Art. 64
CRA	Meldungen seit 11. September 2026; Hauptanforderungen ab 11. Dezember 2027.	Artikel-14-Meldungen betreiben; Produktkonformität und Lebenszyklusnachweise planen. CRA Art. 71 · CRA Art. 69(3)
KI-VO	Allgemein ab 2. August 2026, mit gestaffelten und geänderten Ausnahmen.	Anwendbare Kompetenz-, Verbots-, GPAI- und Transparenzpflichten umsetzen. 2026/1744 Art. 1(40) · KI-VO geändert Art. 4(1)
KI-Hochrisiko	2. Dezember 2027 für relevante Pflichten nach Anhang III; 2. August 2028 für Anhang I.	Geänderten Artikel 113 und Übergangsregeln für Altsysteme prüfen. 2026/1744 Art. 1(40)
KI-Übergang	Bestimmte neue Verbote und Kennzeichnungsübergang für bestehende Systeme: 2. Dezember 2026.	Genauen Anwendungsbereich der Artikel 5 und 50 nach Änderung prüfen. KI-VO geändert Art. 111(4) · 2026/1744 Art. 1(40)
Data Act	Allgemein ab 12. September 2025. Artikel 3(1) erfasst Produkte und verbundene Dienste, die nach dem 12. September 2026 in Verkehr gebracht werden.	Datenzugang durch Gestaltung für neue Produkte prüfen. Data Act Art. 50
Data Act Wechsel	Wechselerntgelte entfallen ab 12. Januar 2027.	Ausstiegsklauseln prüfen; andere zulässige Entgelte unterscheiden. Data Act Art. 29(1)
CER und eIDAS	CER-Fristen hängen von der Einstufungsmitteilung ab. Wallet-Pflichten hängen von Rolle und Durchführungsakten ab.	Tatsächliche Auslöser und Fristen erfassen; kein pauschales Konzerndatum verwenden. CER Art. 6(3) · CER Art. 12(1) · eIDAS Art. 5a(1) · eIDAS Art. 5f

Ergänzende amtliche Quellen

Rechtsgrundlagen [NIS2-Durchführungsverordnung 2024/2690](#) | [DORA-Melderegulierung Verordnung 2025/301](#) | [KI-Änderung 2026/1744](#) | [eIDAS-Änderung 2024/1183](#)

DSGVO und DSA gelten bereits allgemein. Soweit relevant nationale und sektorale Regeln ergänzen. Massgeblich sind die amtlichen Texte; Zuständigkeiten, Tests und Plan zeigen einen praktischen Weg zur Umsetzung der ermittelten Anforderungen.