

Sascha Jung
ADV Konferenz 2. Oktober 2025

**Aktuelle Must-Knows im Cyberbereich -
CRA, NIS 2, DSGVO, AI Act, Data Act**

Überblick



CRA



NIS 2*



DSGVO



AI-Act



Data Act

Was?

Cyberresilienz-
Verordnung

Richtlinie für Netz- und
Informationssicherheit

Datenschutzgrund-
verordnung

Verordnung für Künstliche
Intelligenz

Daten**verordnung**

Adressaten

Hersteller, Händler und
Importeure von
Produkten mit digitalen
Elementen

Unternehmen aus
bestimmten kritischen
Sektoren - jedenfalls
oder bei Erfüllung
bestimmter KPIs (MA,
Umsätze, Bilanzsummen)

Verantwortliche für die
Verarbeitung personen-
bezogener (pb) Daten

Anbieter, Inverkehr-
bringer, Importeure,
Händler und Betreiber
von Produkten oder
Dienstleistungen
basierend auf KI

Hersteller von ver-
netzten Geräten und
verbundenen Diensten

Ziel und Inhalt

Stärkung der
Cybersicherheit von
Produkten mit digitalen
Elementen

Stärkung der Cybersicherheit
von kritischen und digitalen
Diensten durch Etablierung von
Risikomanagementmaßnahmen
und Meldepflichten

Schutz von pb Daten und
Grundrechten
natürlicher Personen
durch Einräumung von
Betroffenenrechten.

Transparenz, Sicherheit
und Schutz von
Grundrechten durch
risikobasierte
Regulierung von KI

Paradigmenwechsel
durch Zuweisung der
Datenhoheit an
NutzerInnen

Umsetzung

Der CRA ist am
11.12.2024 in Kraft
getreten, Meldepflichten
bestehen ab 11.9.2026,
vollständige Anwend-
barkeit mit 11.12.2027

Die NIS-2 ist am
16.1.2023 in Kraft
getreten und hätte bis
17.10.2024 umgesetzt
werden sollen. In
Österreich 2. Entwurf

Die DSGVO ist seit
25.11.2018 anwendbar.

Der AI-Act ist seit
2.2.2025 für verbotene
Systeme und Schulungen,
seit 2.8.2025 für Systeme
mit allg. Verwendungszweck
anwendbar,
vollständige Anwend-
barkeit mit 2.8.2027

Die Datenverordnung
ist seit 12.9.2025
anwendbar

* DORA-VO aufgrund Ähnlichkeit und
Sektorrelevanz hier bewusst ausgelassen

Umsetzungsmaßnahmen



CRA

1. Einhaltung der Grundsätze “Security by Design” oder “Security by Default”
2. Durchführung einer Risikoanalyse
3. Etablierung eines Schwachstellen-managementsystems und eines Meldesystems
4. Dokumentation und Vorbereitung der Konformitätsprüfung



NIS 2

1. Etablierung eines Risikomanagementsystems
2. Einführung der notwendigen technischen und organisatorischen Sicherheitsmaßnahmen
3. Etablierung eines Vorfallmanagementsystems und eines Meldesystems
4. Sicherstellung der Compliance innerhalb der Lieferkette



DSGVO

1. Erstellung einer vollständigen Datenschutzdokumentation (VVZ, Löschkonzept, Datenschutzinformationen, DSFAs, AVVs etc.)
2. Einhaltung der Rechtsgrundlagen und Grundsätze der Datenverarbeitung
3. Etablierung eines Anfragen- und Meldesystems
4. Umsetzung der technischen und organisatorischen Maßnahmen (TOMs)

Steps to take...

Schulung und Sensibilisierung des Personals und Managements

Meldepflichten des Herstellers an den CSIRT und die ENISA und Nutzer gemäß CRA



Was ist eine aktiv ausgenutzte Schwachstelle?

Eine **Schwäche, Anfälligkeit oder Fehlfunktion** eines Produkts mit digitalen Elementen, zu der **verlässliche Nachweise** dafür vorliegen, dass ein böswilliger Akteur sie in einem System ohne Zustimmung des Systemeigners **ausgenutzt hat**

Was ist ein schwerwiegender Sicherheitsvorfall?

- Sicherheitsvorfall, der die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit sensibler oder wichtiger **Daten oder Funktionen beeinträchtigt oder gefährdet**
- ODER
- Sicherheitsvorfall, der dazu führt oder dazu führen könnte, dass **böswilliger Code** in das Produkt mit digitalen Elementen oder in die Netzwerke und Informationssysteme des Nutzers **eingeschleust wird**

Aktiv ausgenutzte
Schwachstelle

Schwerwiegender
Sicherheitsvorfall

1
Frühwarnung (unverzüglich
aber max. 24 h nach Kenntnis)

1
Frühwarnung und
Erklärung zum Verdacht
auf Mutwilligkeit
(unverzüglich aber max. 24 h nach
Kenntnis)

2
Meldung an Behörde (unverzüglich
aber max. 72 h nach Kenntnis)
+ Zwischenbericht wenn
angefordert

Meldung an Nutzer (nach Kenntnis)

3
Abschlussbericht
(14 Tage nach Bereitstellung einer
Korrekturmaßnahme)

3
Abschlussbericht
(1 Monat nach Meldung;)

Sofern der Sicherheitsvorfall auch die Verletzung
personenbezogener Daten umfasst gilt zusätzlich
das Melderegime der DSGVO



Inhalt der Meldung bzw. des Abschlussberichts

Information insbesondere zu

- Mitgliedstaaten, in deren Hoheitsgebiet das Produkt bereitgestellt wurde
- dem betreffenden Produkt
- dem Verdacht, dass der Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist
- der allgemeinen Art der Ausnutzung und der betreffenden Schwachstelle bzw. die Art des Sicherheitsvorfalls
- dem Schweregrad und Auswirkungen der betreffenden Schwachstelle bzw. des Sicherheitsvorfalls
- allen ergriffenen und laufenden Korrektur- oder Risikominderungsmaßnahmen
- Korrektur- oder Abhilfemaßnahmen, die Nutzer ergreifen können
- der Einstufung der Sensibilität der gemeldeten Informationen
- der Schwachstelle, einschließlich ihres Schweregrads und ihrer Auswirkungen

Meldepflichten der Einrichtung an den CSIRT / die zuständige Behörde gemäß NIS 2



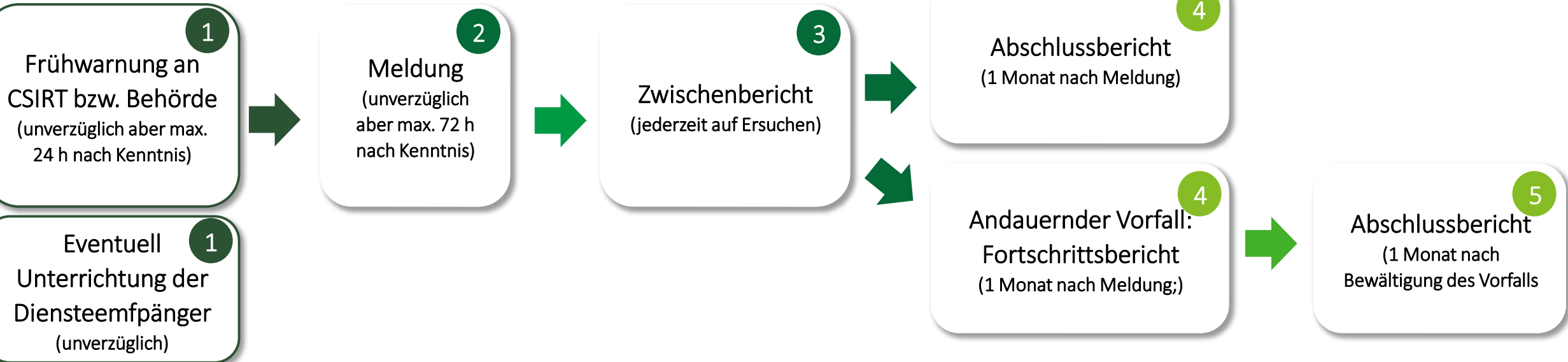
Was ist ein erheblicher Sicherheitsvorfall?

Sicherheitsvorfall, der

- **schwerwiegende** Betriebsstörungen der Dienste / finanzielle Verluste für die Einrichtung verursacht hat / verursachen kann

oder

- andere natürliche / juristische Personen durch **erhebliche** materielle / immaterielle Schäden beeinträchtigt hat / beeinträchtigen kann



Sofern der Sicherheitsvorfall auch die Verletzung personenbezogener Daten umfasst gilt zusätzlich das Melderegime der DSGVO



Inhalt der Meldung bzw. des Abschlussberichts

Information insbesondere zu

- dem Verdacht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte
- der Bewertung und Beschreibung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren
- der Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat
- den getroffenen und laufenden Abhilfemaßnahmen
- den gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls

Meldepflichten des Verantwortlichen an die DSB und die Betroffenen gemäß DSGVO



Was ist eine Verletzung des Schutzes personenbezogener Daten?

eine **Verletzung der Sicherheit**, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden

Was ist das Risiko für die Rechte und Freiheiten natürlicher Personen?

- Die Höhe des Risikos bemisst sich insbesondere nach der **Art** der Datenschutzverletzung, dem **Umgang und der Art** der betroffenen Daten, der **Identifizierbarkeit** und **Anzahl** der betroffenen Personen, die **Schwere der Folgen** der Verletzung
- Rechte und Freiheiten sind berührt etwa infolge Verlust der Datenkontrolle, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile

Datenschutzverletzung voraussichtlich ohne Risiko für die Rechte und Freiheiten nat. Personen



Keine Meldung

1

Datenschutzverletzung mit Risiko für die Rechte und Freiheiten nat. Personen



Meldung an die Datenschutzbehörde (unverzüglich aber max. 72 h nach Kenntnis)

1

Datenschutzverletzung mit voraussichtlich hohem Risiko für die Rechte und Freiheiten nat. Personen



Meldung an die betroffenen natürlichen Personen (unverzüglich nach Kenntnis)

1

Meldepflichten des Verantwortlichen an die DSB und die Betroffenen gemäß DSGVO



Inhalt der Meldung

Information insbesondere zu

- der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- den Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- den wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- den ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- dem Grund, warum allenfalls die betroffenen Personen nicht zu informieren sind

Wir stehen Ihnen gerne als Ansprechpartner zur Verfügung
Ihr Deloitte Legal Data Protection | Cybersecurity Team

Hauptansprechpartner:



Sascha Jung
Rechtsanwalt, Partner

+43 676 626 9912
s.jung@jankweiler.at



Christian Kern
Rechtsanwalt, Senior Manager

+43 660 666 0046
c.kern@jankweiler.at

www.jankweiler.at
www.deloitte.com/at/de/services/legal

