Bettina Sterner, BA

Regulatory Cheat Sheet – DSGVO, CRA, KI-VO, NIS2/NISG

Stand: März 2026 · Österreich / EU · Kein Ersatz für Rechtsberatung im Einzelfall · Anwendbarkeit ist stets projektspezifisch zu prüfen

	DSGVO	Cyber Resilience Act (CRA)	KI-Verordnung (KI-VO)	NIS-2-Richtlinie / NISG 2026
Zweck	Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten	Cybersicherheit von Produkten mit digitalen Elementen (= Software- oder Hardwareprodukt inkl. Datenfernverarbeitungslösungen, Art 3 Z 1 CRA) über den gesamten Lebenszyklus, inkl. nach Inverkehrbringen	Sicherheit, Transparenz und Vertrauenswürdigkeit von KI-Systemen (= maschinenbasiertes System, das auf Grundlage von Eingaben Ausgaben wie Vorhersagen, Empfehlungen oder Entscheidungen erzeugt, Art 3 Z 1 KI-VO). Daneben eigene Regelungen für KI-Modelle mit allgemeinem Verwendungszweck (GPAI, Art 3 Z 63 KI-VO)	Hohes gemeinsames Cybersicherheitsniveau in der EU; Schutz wesentlicher und wichtiger Einrichtungen (inkl. öffentlicher Stellen) und deren Dienste
Adressaten	**Verantwortlicher iSd DSGVO** (Art 4 Z 7 DSGVO): bestimmt allein oder gemeinsam Zwecke und Mittel der Verarbeitung **Auftragsverarbeiter iSd DSGVO** (Art 4 Z 8 DSGVO): verarbeitet pb Daten ausschließlich im Auftrag und auf Weisung → verpflichtender Vertrag (Art 28 DSGVO) **Gemeinsam Verantwortliche iSd DSGVO** (Art 26 DSGVO): bestimmen gemeinsam Zwecke und Mittel → Vereinbarung erforderlich	**Hersteller** (Art 3 Z 13 CRA): bringt Produkt unter eigenem Namen in Verkehr — ausgelagerte Entwicklung schadet der Herstellerqualifikation nicht zwingend **Importeure** (Art 3 Z 19 CRA): bringen Produkt eines Drittland-Herstellers in Verkehr **Händler** (Art 3 Z 20 CRA): stellen Produkt auf dem Markt bereit ohne es wesentlich zu verändern	**Anbieter** (Art 3 Z 3 KI-VO): entwickelt KI-System oder lässt es entwickeln und bringt es unter eigenem Namen in Verkehr **Betreiber** (Art 3 Z 4 KI-VO): setzt KI-System in eigener Verantwortung ein Importeure, Händler, Bevollmächtigte	**Wesentliche Einrichtungen** (Anhang I NIS2-RL): Energie, Verkehr, Bankwesen, Gesundheit, digitale Infrastruktur u.a. **Wichtige Einrichtungen** (Anhang II NIS2-RL): Post, Abfallwirtschaft, Lebensmittel, Forschung u.a. Größenschwellen: ≥50 MA oder ≥€10 Mio. Umsatz Behörde kann Einrichtung unabhängig von Größe als wesentlich einstufen Gilt auch für öffentliche Stellen
Betroffene	Natürliche Personen iSd Art 4 Z 1 DSGVO: jede Information, die sich auf eine identifizierte oder identifizierbare natürliche Person bezieht — der Begriff wird sehr weit ausgelegt	Nutzerinnen und Nutzer von Produkten mit digitalen Elementen (Verbraucher und Unternehmen)	Natürliche Personen, die von KI-Systemen betroffen sind	Gesellschaft; Nutzerinnen und Nutzer wesentlicher und wichtiger Dienste

	DSGVO	Cyber Resilience Act (CRA)	KI-Verordnung (KI-VO)	NIS-2-Richtlinie / NISG 2026
Wann anwendbar	Bei jeder Verarbeitung (= jeder Vorgang im Zusammenhang mit pb Daten, Art 4 Z 2 DSGVO: Erheben, Erfassen, Speichern, Verwenden, Übermitteln, Löschen u.v.m.) pb Daten. Räumlicher Anwendungsbereich: Art 3 DSGVO. Risikobeurteilung: Einzelfallbewertung abhängig von Art, Umfang, Zwecken und Umständen der Verarbeitung — kein starres Risikostufensystem.	Bei Inverkehrbringen von Produkten mit digitalen Elementen. Zwei Kategorien: **Standard:** alle sonstigen Produkte **Kritisch:** Anhang III + IV (Betriebssysteme, Firewalls, Smartcards u.a.) → erhöhte Anforderungen	Bei Entwicklung oder Einsatz von KI-Systemen iSd Art 3 Z 1 KI-VO: **Verboten:** inakzeptables Risiko (Art 5 KI-VO) **Hochrisiko:** Art 6 iVm Anhang III KI-VO **Begrenzt:** Transparenzpflichten (Art 50 KI-VO) **Minimal:** keine besonderen Pflichten	Kein dezidiertes Risikolevel: Art 21 Abs 1 NIS2-RL verlangt geeignete und verhältnismäßige Maßnahmen auf Basis eines verpflichtenden Risk Assessments — bewegliches System.
Geltungs-beginn	**25. Mai 2018** (vollständig in Kraft)	In Kraft seit Dezember 2024 (gestaffelt): **11.6.2026** → Notifizierung und Konformitätsbewertung **11.09.2026** → Meldepflichten für Hersteller **11.12.2027** → vollständige Anwendung **Art 69 CRA:** Übergangsregelungen für Produkte, die vor dem 11.12.2027 in Verkehr gebracht werden	In Kraft ab 2. August 2026 (gestaffelt): **allerdings grace periods bzw. früherer Gültigkeitsbeginn** **02.02.2025** → verbotene Praktiken **02.08.2025** → GPAI-Modelle; Art 4 KI-VO (Anbieter und Betreiber müssen ausreichende KI-Kompetenz ihres Personals sicherstellen — bereits in Kraft) **02.08.2026** → Hochrisiko (Anh. III) **02.08.2027** → vollständige Anwendung	NIS2-RL: seit Januar 2023 in Kraft **NISG 2026 (AT): ab 01.10.2026**
Security-Anforderungen	**Art 25 DSGVO:** Privacy by Design & Default **Art 32 DSGVO:** Geeignete TOMs unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung und der Eintrittswahrscheinlichkeit und Schwere des Risikos — laufend zu überwachen und zu überprüfen	Anforderungen nach Anhang I CRA (gestaffelt nach Produktkategorie), u.a.: Security by Design, Vulnerability Management, SBOM, keine bekannten ausgenutzten Schwachstellen bei Inverkehrbringen, Sicherheitsupdates mind. 5 Jahre (kürzer, falls Nutzungsdauer 5 Jahre nicht überschreitet)	Gestaffelt nach Risikoklasse; für Hochrisiko-KI insb.: Art 10 (Datengovernance & Bias-Prüfung), Art 11 (Techn. Dokumentation, Aufbewahrung mind. 10 Jahre), Art 12 (Protokollierung), Art 13 (Transparenz), Art 14 (Menschliche Aufsicht), Art 15 (Genauigkeit, Robustheit, Cybersicherheit), Konformitätsbewertung vor Inverkehrbringen, Art 49 (Registrierung in EU-Datenbank)	Art 21 Abs 1 NIS2-RL: gefahrenübergreifender Ansatz, der zumindest die in Art 21 Abs 2 NIS2-RL genannten Bereiche umfasst (u.a. Risikoanalyse, Incident Handling, BCM, Supply Chain Security, Verschlüsselung, Zugriffskontrolle, MFA, Schulung). Betrifft die gesamte Einrichtung.

	DSGVO	Cyber Resilience Act (CRA)	KI-Verordnung (KI-VO)	NIS-2-Richtlinie / NISG 2026
Meldepflichten	**Art 33 iVm Art 4 Z 12 DSGVO:** Verletzung des Schutzes pb Daten → unverzüglich, spätestens 72h nach Kenntnis **Art 34 DSGVO:** Informationspflicht gegenüber Betroffenen bei voraussichtlich hohem Risiko für deren Rechte und Freiheiten	**Aktiv ausgenutzte Schwachstelle** + **schwerwiegender Sicherheitsvorfall** (= Vorfall mit erheblichen Auswirkungen auf Verfügbarkeit, Integrität oder Vertraulichkeit): **24h** Frühwarnung → ENISA / nat. Behörde **72h** Meldung **14 Tage** Abschlussbericht	**Schwerwiegender Vorfall** (Art 3 Z 49 KI-VO) + **Fehlfunktion**: **15 Tage ab Kenntnis** an Marktüberwachungsbehörde (Art 73 KI-VO; im Fall des Todes einer Person früher – binnen 10 Tagen) Betreiber → melden unverzüglich an Anbieter	**Erheblicher Cybersicherheitsvorfall** (Art 23 Abs 3 NIS2-RL: schwerwiegende Betriebsstörungen / finanzielle Verluste oder erhebliche materielle / immaterielle Schäden für Dritte): **24h** Frühwarnung **72h** Meldung **auf Anfrage** Zwischenbericht **1 Monat** Abschlussbericht → zuständiges CSIRT
Strafrahmen (max)	Abhängig vom Tatbestand (z.B. Verletzung von Betroffenenrechten, unzulässiger Drittlandtransfer, Verstöße gegen Art 5 DSGVO): bis **€20 Mio.** oder **4%** des weltweiten Jahresumsatzes	Gestaffelt (Art 64 CRA): Verstöße Anhang I: bis **€15 Mio.** oder **2,5%** Andere Verstöße: bis **€10 Mio.** oder **2%** Falschaussagen: bis **€5 Mio.** oder **1%** (jeweils des weltweiten Jahresumsatzes)	Gestaffelt: Verbotene Praktiken (Art 5): bis **€35 Mio.** oder **7%** Anbieterpflichten (Art 16): bis **€15 Mio.** oder **3%** Falschaussagen: bis **€7,5 Mio.** oder **1%** (jeweils des weltweiten Jahresumsatzes)	Verstöße gegen Art 21 NIS2-RL: Wesentliche Einrichtungen: bis **€10 Mio.** oder **2%** Wichtige Einrichtungen: bis **€7 Mio.** oder **1,4%** (jeweils des weltweiten Jahresumsatzes) Andere Verstöße mit weiteren (anderen) Strafrahmen