EIWTC SECURITY ADVISORY

Security · Resilience · Technical Consulting

WISSEN FÜR PLANUNG UND BETRIEB

Cyber Resilience Act

Sichere Produkte. Verlässlicher Betrieb.

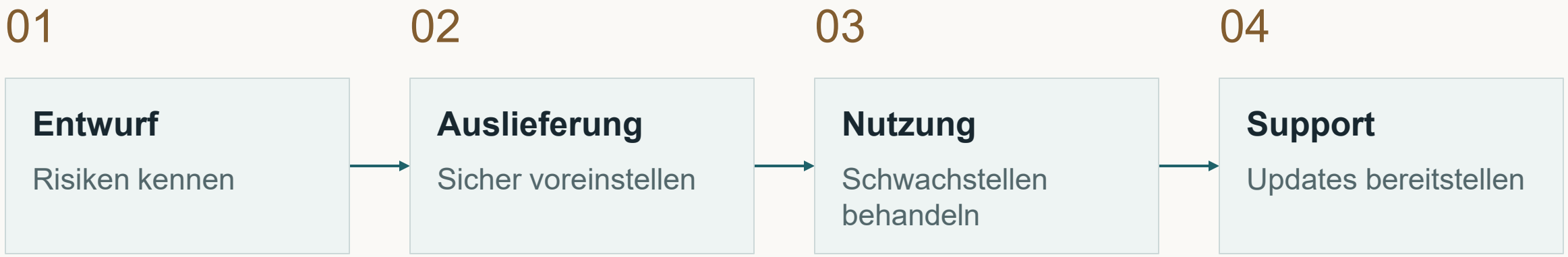


KI-Illustration · fiktive Szene

Verordnung (EU) 2024/2847 · Aktualisiert 19. November 2026

Sicherheit gehört von Anfang an zum Produkt.

Der Podcast startet mit einer Frage: Würden wir ein Auto ohne Bremsen akzeptieren?



Der CRA verankert Cybersicherheit über den Produktlebenszyklus.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

DAS BEISPIEL AUS DEM PODCAST

Smart Baby 3000

Eine kleine Kamera.
Ein sehr privater Raum.

- Kamera im Kinderzimmer
- App auf dem Smartphone
- Cloud-Dienst des Herstellers



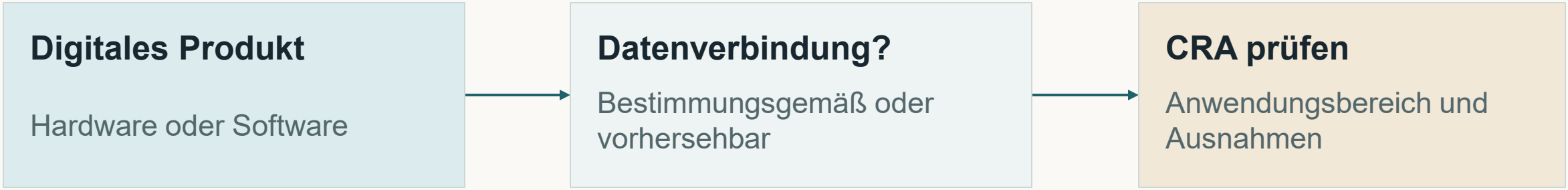
KI-Illustration · fiktive Szene

Podcast 01:49–03:54 · fiktives Produkt

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Die Datenverbindung ist der erste Prüfpunkt.

Direkt oder indirekt. Mit einem Gerät oder einem Netz.



Auch ohne Internet: Digitale Daten mit Identmedium oder Programmiergerät können genügen.

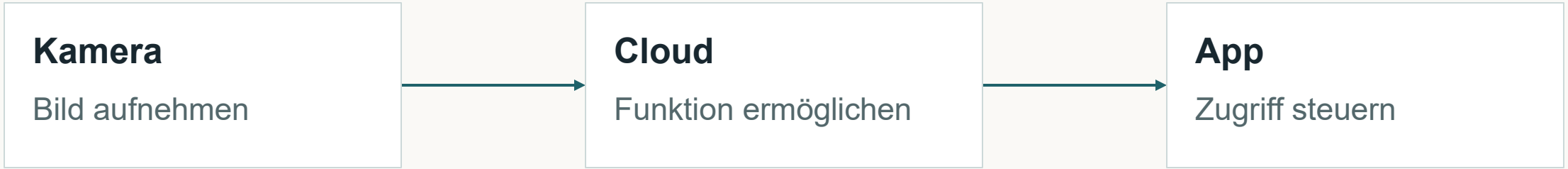
Ein rein mechanisches Schloss liegt außerhalb dieses digitalen Produktbegriffs.

CRA Art. 2–3 · Leitlinien Rn. 26–28 · EIWTC-Anwendungsbeispiel

Die Cloud kann zum Produkt gehören.

Drei Kriterien ordnen die Fernverarbeitung dem Produkt zu.

BEISPIEL: SMART BABY 3000 MIT ZUGEHÖRIGER CLOUD



1. **Entfernte Datenverarbeitung**
2. **Ohne sie fällt mindestens eine Produktfunktion aus.**
3. **Softwareentwicklung durch den Hersteller oder unter seiner Verantwortung.**

CRA Art. 3 Nr. 1–2 · Leitlinien Rn. 184, 189, 202

Sicher vom ersten Start an.

Die Risikobewertung bestimmt die konkrete Umsetzung.

01	**Zugriff schützen**	Unbefugte Zugriffe verhindern.
02	**Daten begrenzen**	Nur die für den Zweck nötigen Daten verarbeiten.
03	**Lücken behandeln**	Ohne bekannte ausnutzbare Schwachstellen bereitstellen.
04	**Sicher beenden**	Daten und Einstellungen einfach und sicher löschen.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Die Lieferkette muss Sicherheit mittragen.

Auch wenn der Hersteller außerhalb der EU sitzt.

Hersteller
Bewerten und nachweisen

→

Einführer
Nachweise vorab prüfen

→

Händler
Kennzeichnung prüfen und handeln

Eigene Marke oder wesentliche Änderung können eine Herstellerrolle auslösen.

CRA Art. 13, 19–22 · Podcast 05:54–06:55

Freier Code bleibt Teil der Produktverantwortung.

Das Babyphone nutzt eine Open-Source-Kamerabibliothek.

Freie Entwicklung

Außerhalb einer Geschäftstätigkeit

→

Kommerzielles Produkt

Hersteller prüft integrierte Komponenten

Keine pauschalen Herstellerpflichten für freie Entwicklung.

Die Verantwortung für das Endprodukt bleibt beim Hersteller.

Open-Source-Verwalter

Eigene, angepasste Pflichten für systematische Unterstützung.

CRA Art. 13 Abs. 5–6, Art. 24 · Erwägungsgründe 18–19

Support folgt der erwartbaren Nutzung.

Der Hersteller begründet den Zeitraum für das konkrete Produkt.

Regel und Ausnahme

Mindestens fünf Jahre.
Bei kürzerer Nutzung
gilt deren erwartete Dauer.

Längere Nutzung

Ein längerer Lebenszyklus
verlangt einen entsprechend
längeren Support.

Konkretes Supportende

Mindestens Monat und Jahr.
Für Käufer beim Kauf
klar erkennbar.

Die Zusage muss zum vorgesehenen Produktlebenszyklus passen.

CRA Art. 13 Abs. 8–9, 19 · Leitlinien C/2026/6013, Rn. 125–135

Ein Sicherheitsupdate muss sicher ankommen.

Grundsätzlich unverzüglich und kostenlos.

01 **Bereitstellen**
Schwachstelle beheben

→

02 **Verteilen**
Sicherer Updatekanal

→

03 **Installieren**
Automatisch, soweit zutreffend

→

04 **Weiter nutzen**
Funktion erhalten

Sicherheits- und Funktionsupdates trennen, soweit technisch machbar.

CRA Anhang I Teil I Nr. 2 c, Teil II Nr. 2, 7–8

Die SBOM zeigt, wo eine verwundbare Zutat steckt.

Software-Stückliste: maschinenlesbar, mit zumindest den obersten Abhängigkeiten.



Komponenteninfos gezielt nutzen.

CRA Anhang I Teil II Nr. 1 · Anhang II Nr. 9

CE braucht eine nachvollziehbare Grundlage.

Die Kennzeichnung umfasst künftig auch die anwendbaren CRA-Anforderungen.

01

Risikoanalyse

Produkt und Verwendung

02

Dokumentieren

Technische Unterlagen

03

Bewerten

Passender Konformitätsweg

04

Erklären

EU-Konformität und CE

CE ist kein Versprechen absoluter Sicherheit.

CRA Art. 28–32 · Podcast 14:36–16:23

Die Produktkategorie bestimmt den Prüfweg.

Kategorie	Beispiele	Konformitätsweg
Regulärer Fall	Nicht in Anhang III / IV	Interne Kontrolle ist möglich.
Wichtig: Klasse I	Babyphone, Smart-Home-Schlösser, Authentifizierungsleser*	Drittprüfung, wenn geeignete Referenzen nicht vollständig angewandt werden.
Wichtig: Klasse II	Firewalls, Container-Runtimes	Drittbewertung oder zulässiger Zertifizierungsweg.
Kritisch	Smart-Meter-Gateways, bestimmte Sicherheitsgeräte	Art. 8 oder Verfahren nach Art. 32.

***Kernfunktion und konkrete technische Beschreibung entscheiden.**

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Unverzüglich melden, spätestens in 24 Stunden.

Bei Kenntnis aktiver Ausnutzung oder eines schwerwiegenden Sicherheitsvorfalls am Produkt.

Kenntnis
Startpunkt der Fristen

→

24 h
Frühwarnung

→

72 h
Meldung mit verfügbaren Details

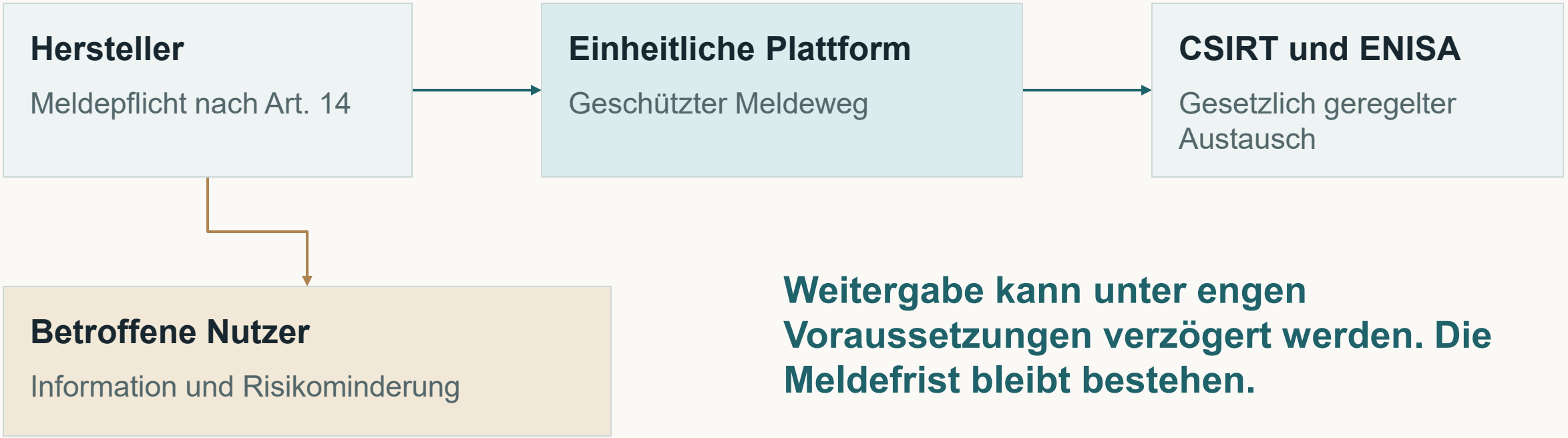
ABSCHLUSSBERICHT

Schwachstelle
Spätestens 14 Tage nach verfügbarer Abhilfe.

Vorfall
Innerhalb eines Monats nach der 72-h-Meldung.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Geschützt melden. Betroffene Nutzer informieren.



Weitergabe kann unter engen Voraussetzungen verzögert werden. Die Meldefrist bleibt bestehen.

CRA Art. 14 Abs. 8, Art. 16, 63

Die Regeln haben wirtschaftliche Folgen.

Für bestimmte Verstöße gelten hohe Bußgeldobergrenzen.

15 Mio. €

oder 2,5 % des weltweiten Jahresumsatzes

Der höhere Betrag zählt.

Auch der Marktzugang ist betroffen.

Korrekturen
Vertrieb beschränken
Rückrufe

CRA Art. 54, 58, 64 · Podcast 20:06–21:47

Meldepflichten gelten bereits. Hauptpflichten folgen.

Drei Daten machen den Übergang sichtbar.

10.12.2024

Inkrafttreten

Teil des EU-Rechts

11.09.2026

Meldepflichten

Art. 14 gilt bereits

11.12.2027

Hauptpflichten

Produktanforderungen und Konformität

Seit 11.06.2026: Vorschriften zur Notifizierung von Bewertungsstellen.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Die Kommission präzisiert die Anwendung.

Offizielle Auslegungshilfe zum bestehenden Cyber Resilience Act.

17.11.2026

C/2026/6013

67 Praxisbeispiele
24 EU-Amtssprachen

Rechtlich nicht bindend

Die Leitlinien erläutern Produktgrenzen, Support, Änderungen und Meldungen.

Anwendungstermine bleiben bestehen

11.09.2026 Herstellermeldungen
11.12.2027 Allgemeine Anwendung

Kommissionsmitteilung, Rn. 6–8 · Kommissionsmeldung aktualisiert am 18.11.2026

Bestand: Änderung und Meldung getrennt prüfen.

Maßgeblich ist das Inverkehrbringen, nicht allein das Kaufdatum.

Vor 11.12.2027
Bereits in Verkehr gebracht

→

Ab 11.12.2027
Wesentliche Änderung?

→

Hauptpflichten
Einzelfall prüfen

Art. 14 gilt auch für ältere Produkte und nach Supportende. Meldepflichten bei Kenntnis einschlägiger Ereignisse beachten.

CRA Art. 69 Abs. 2–3 · Leitlinien Rn. 210, 217

Wann wird eine Änderung wesentlich?

Entscheidend sind Zweckbestimmung und Auswirkungen auf die Konformität.

Im bewerteten Rahmen

Vorgesehene Reparatur, Konfiguration und Fehlerbehebung sind nicht automatisch wesentlich.

Neue Funktion oder neues Risiko

Neue Fernöffnung, Cloud-Anbindung oder externe Schlüsselverwaltung: Auswirkungen im Einzelfall bewerten.

Mögliche Herstellerrolle

Wesentlich ändern und anschließend auf dem Markt bereitstellen: Herstellerpflichten nach Art. 22 prüfen.

CRA Art. 3 Nr. 30, Art. 21–22 · Leitlinien Abschnitt 4 · Hauptpflichten ab 11.12.2027

Produktsicherheit und Haftung ergänzen sich.

CRA Produktanforderungen, Konformität und Schwachstellenbehandlung

Ersatzanspruch

Produktfehler + **Ersatzfähiger Schaden** + **Kausalität**

Ein fehlendes Update bedeutet nicht automatisch Ersatz jedes IT-Schadens.

CRA Erwägungsgrund 31 · Richtlinie (EU) 2024/2853

Digitale Sicherheit entscheidet mit, wer hinein darf.

Wer erhält Zutritt?

Leser prüfen Identitäten.
Steuerungen geben Türen frei.
Software verwaltet Rechte.



KI-Illustration · fiktive Szene

EIWTC-Anwendungsbeispiel · Anhang III Klasse I Nr. 1 · VO (EU) 2025/2392

Ein Update muss auch im Gebäude funktionieren.

Illustratives Beispiel: Eine Schwachstelle betrifft die Zutrittssoftware.

01 **Bestand abgleichen**

Betroffene Versionen erkennen

02 **Abhilfe abstimmen**

Risiko und Wartungsfenster klären

03 **Aktualisieren und prüfen**

Türfunktionen und Wiederanlauf testen



KI-Illustration · fiktive Szene

Illustratives EIWTC-Betriebsbeispiel

Herstellerinformationen für einen sicheren Betrieb

Information des Herstellers	Nutzen für Planung und Betrieb
Produkt, Version und Systemgrenzen	Komponenten und Cloud-Abhängigkeiten kennen
Supportende und Unterstützungsumfang	Verbleibenden Support und Migration planen
Sicherheitsupdates und Updateweg	Verantwortung und Wartungsfenster klären
Konformität und Bewertungsverfahren	Anwendbare Produktnachweise einordnen
Sicherheitskontakt und Warnungen	Betroffenheit prüfen und Maßnahmen abstimmen

Klare Produktinformationen unterstützen einen verlässlichen Betrieb.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Zuerst die Funktion. Dann die Technik.

Nutzung und Schutzziele führen zu Anforderungen an Produkte, Schnittstellen und Betrieb.

Nachweise und Updates gehören in die Planung.



KI-Illustration · fiktive Szene

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Der nächste Schritt ist ein klarer Arbeitsablauf.

Eine verantwortliche Person hält offene Punkte und Fristen zusammen.

Bestand erfassen

Versionen, Cloud, Supportende

→

Verantwortung klären

Herstellerkontakt und Updateablauf

→

Abläufe erproben

Warnung, Entscheidung, Update

So werden aus Produktinformationen belastbare Entscheidungen.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting



Sicherheit wird Teil der Produktqualität.

Vom Entwurf bis zum Support.
Nachvollziehbar für Hersteller und Betreiber.

Sicherheit im Produkt. Klarheit in der Planung.

KI-Illustration · fiktive Szene

eiwtc.lu/de/security/

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Quellen und Einordnung

Rechtsgrundlage	Verordnung (EU) 2024/2847: Anforderungen und Anwendungstermine.
Produktkategorien	VO (EU) 2025/2392: verbindliche technische Beschreibungen.
Auslegungshilfe	C/2026/6013 vom 17.11.2026: rechtlich nicht bindende Leitlinien.
Kommissionsmeldung	67 Praxisbeispiele, 24 Amtssprachen. Aktualisiert am 18.11.2026.
Produkthaftung	Richtlinie (EU) 2024/2853: gesonderte Haftungsregelung.

Podcast als Erzählvorlage und weitere Quellen in den Notizen. Stand 19.11.2026.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting