

EU-Regeln für vernetzte Produkte und Industrieteile

Warum Compliance jetzt Pflicht ist — ein Leitfaden für Einkauf, Importeure und Betreiber (Stand Oktober 2026)

ITDA-S — ein Unternehmen von QmiSoft · www.itda-s.com

Oktober 2026

Warum das jetzt wichtig ist

Zwischen Dezember 2024 und Jänner 2027 setzt die Europäische Union eine Reihe neuer Produktregeln in Kraft. Gemeinsam verändern sie eines grundlegend: **Wer ein Produkt auf dem EU-Markt in Verkehr bringt, ist für seine Sicherheit, seine Cybersicherheit und seine Dokumentation verantwortlich — über Jahre nach der Lieferung.**

Für alle, die Elektronik, Sensoren, Automatisierungsteile oder vernetzte Geräte außerhalb der EU einkaufen, heißt das:

- **Der Importeur trägt herstellerähnliche Pflichten.** Wer direkt bei einer Fabrik in Asien kauft und das Produkt in die EU bringt, ist Importeur — mit eigenen gesetzlichen Pflichten.
- **Cybersicherheit ist jetzt Teil der Produktkonformität.** Ein vernetztes Gerät, das sich nicht aktualisieren lässt, Standardpasswörter hat oder keinen Umgang mit Schwachstellen vorsieht, kann nicht konform sein — auch wenn es einwandfrei funktioniert.
- **Die Dokumentation muss vorliegen, bevor die Ware in Verkehr gebracht wird** — und bis zu 10 Jahre aufbewahrt werden.
- **Behörden können Produkte stoppen.** Marktüberwachung und Zoll können nicht konforme Produkte zurückhalten, vom Markt nehmen oder zurückrufen. Bußgelder nach der Cyberresilienz-Verordnung reichen bei den schwersten Verstößen bis zu 15 Mio. € oder 2,5 % des weltweiten Jahresumsatzes.

Die Regeln im Überblick

Regelwerk	Gilt seit / ab	Betrifft	Kernpflicht
Allgemeine Produktsicherheitsverordnung (GPSR), VO (EU) 2023/988	13.12.2024	Alle Verbraucherprodukte	In der EU niedergelassener Wirtschaftsakteur, Produktkennzeichnung, Sicherheitsdokumentation, Meldung von Unfällen
Funkanlagenrichtlinie — Cybersicherheit,	1.8.2025 (bis 11.12.2027, danach	Internetfähige Funkanlagen (WLAN,	Schutz des Netzes, Schutz

Regelwerk	Gilt seit / ab	Betrifft	Kernpflicht
Delegierte VO (EU) 2022/30 (harmonisierte Normen EN 18031)	durch den CRA abgedeckt)	Mobilfunk, Bluetooth, LoRa ...)	personenbezogener Daten, Schutz vor Betrug
Batterieverordnung (EU) 2023/1542 — Herstellerverantwortung	18.8.2025	Batterien, auch in Geräten verbaut	Herstellerregistrierung in jedem Mitgliedstaat, Kennzeichnung, Rücknahme
Datenverordnung (Data Act), VO (EU) 2023/2854	12.9.2025; Gestaltungspflicht für nach dem 12.9.2026 in Verkehr gebrachte Produkte	Vernetzte Produkte und verbundene Dienste	Nutzer über erzeugte Daten informieren; Zugang zu ihren Daten gewähren
Cyberresilienz-Verordnung (CRA), VO (EU) 2024/2847	Konformitätsbewertungsstellen 11.6.2026 · Meldepflicht 11.9.2026 · volle Anwendung 11.12.2027	Nahezu alle Produkte mit digitalen Elementen (Hard- und Software)	Sicherheit ab Entwurf, Schwachstellenmanagement, Sicherheitsupdates im Unterstützungszeitraum, CE-Kennzeichnung, Meldung ausgenutzter Schwachstellen binnen 24 h / 72 h
Österreichisches NIS2-Gesetz (NISG 2026)	In Kraft seit 1.10.2026; Registrierung bis 31.12.2026	Größere Unternehmen (ab 50 Beschäftigten oder 10 Mio. €) in 18 Sektoren	Risikomanagement, Meldung von Vorfällen, Sicherheit der Lieferkette — wird an Lieferanten weitergegeben
Neue Produkthaftungsrichtlinie (EU) 2024/2853	Nationale Umsetzung bis 9.12.2026	Alle Produkte inkl. Software	Verschuldensunabhängige Haftung auch für Software und fehlende Sicherheitsupdates; Importeure haften, wenn der Hersteller außerhalb der EU sitzt
Maschinenverordnung (EU) 2023/1230	20.1.2027	Maschinen und verbundene Produkte	Ersetzt die Maschinenrichtlinie; Schutz sicherheitsrelevanter Funktionen vor Manipulation (Cybersicherheit), digitale Betriebsanleitungen

Ebenfalls relevant beim Import: Elektroaltgeräteverordnung (Herstellerregistrierung im EDM), RoHS, Verpackungslizenz, EU-Exportkontrolle für Dual-Use-Güter und Sanktionsprüfung.

Schwerpunkt: die Cyberresilienz-Verordnung (CRA)

Der CRA ist das erste horizontale EU-Gesetz, das Cybersicherheit zur Voraussetzung für den Verkauf jedes Produkts mit digitalen Elementen macht — vom smarten Sensor über die SPS mit Netzwerkschnittstelle bis zur Software, die darauf läuft.

Was Hersteller tun müssen:

1. Cyberrisiken bewerten und das Produkt sicher gestalten (keine bekannten ausnutzbaren Schwachstellen, sichere Standardkonfiguration, Schutz der Daten, minimale Angriffsfläche).
2. Schwachstellen managen: eine Meldestelle, eine Software-Stückliste (SBOM), kostenlose Sicherheitsupdates im Unterstützungszeitraum (in der Regel mindestens fünf Jahre).
3. Alles in einer technischen Dokumentation und einer EU-Konformitätserklärung festhalten; CE-Kennzeichnung anbringen.
4. Seit 11. September 2026: aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle melden — Frühwarnmeldung binnen 24 Stunden, Meldung binnen 72 Stunden.

Was Importeure und Händler tun müssen:

- **Importeure** dürfen nur Produkte in Verkehr bringen, deren Hersteller die Anforderungen erfüllt hat: Konformitätsbewertung durchgeführt, technische Dokumentation vorhanden, CE-Kennzeichnung angebracht, Kontaktdaten und Unterstützungszeitraum angegeben. Sie müssen ihren eigenen Namen und ihre Anschrift angeben, die Dokumentation für Behörden bereithalten und den Hersteller über bekannt gewordene Schwachstellen informieren.
- **Händler** prüfen CE-Kennzeichnung, mitgelieferte Informationen und Unterstützungszeitraum — und dürfen Produkte, die sie als nicht konform kennen, nicht verkaufen.
- **Wer ein Produkt wesentlich verändert** oder unter eigenem Namen oder eigener Marke verkauft, gilt selbst als Hersteller.

Produktklassen: Für die meisten Produkte genügt eine Selbstbewertung. „Wichtige“ Produkte (Klasse I und II, z. B. Router, Mikrocontroller mit Sicherheitsfunktionen, Firewalls) können eine Bewertung durch Dritte erfordern; „kritische“ Produkte können eine europäische Cybersicherheitszertifizierung erfordern, sobald ein delegierter Rechtsakt dies vorschreibt.

Was das in der Praxis bedeutet

Wenn Sie ...	dann müssen Sie ...
vernetzte Geräte oder Komponenten aus Asien importieren	als Importeur handeln: Dokumentation, CE-Kennzeichnung, EN-18031-/CRA-Status prüfen, Unterlagen 10 Jahre aufbewahren
Teile in eine Maschine oder Anlage integrieren	sicherstellen, dass das Gesamtsystem konform ist — ab 2027 inklusive Cybersicherheit nach der Maschinenverordnung
als größeres Unternehmen Anlagen betreiben (NIS2)	von Lieferanten Sicherheitsnachweise und Update-Zusagen verlangen
vernetzte Produkte verkaufen	Käufer über die vom Produkt erzeugten Daten informieren (Data Act)
Anlagen 10 Jahre und länger betreiben	Ersatzteile, Sicherheitsupdates und Alternativen von Anfang an einplanen

Checkliste vor dem Kauf eines vernetzten Teils:

- ☐ Wer ist Hersteller, wer ist EU-Wirtschaftsakteur?
- ☐ EU-Konformitätserklärung und Prüfberichte vorhanden?
- ☐ RED-/EN-18031-Status für Funkmodule?
- ☐ Festgelegter Unterstützungszeitraum und Update-Politik (CRA)?
- ☐ SBOM und Kontakt für Schwachstellenmeldungen?
- ☐ Data-Act-Informationen zu den erzeugten Daten?
- ☐ Exportkontrolle, Batterie- und Elektroaltgeräte-Registrierung geklärt?
- ☐ Alternativprodukt für den Fall einer Abkündigung?

Wie ITDA-S hilft — EU-Ready by ITDA-S

ITDA-S übernimmt die ganze Kette für Teile aus Asien und Europa: **Beschaffen** → **EU-Ready machen** → **Integrieren** → **Absichern**.

- **EU-Ready-Akte je Artikel:** Datenblatt, Konformitätserklärung, Prüfberichte, RED-/EN-18031- und CRA-Status, Wirtschaftsakteur.
- **Risikostufe und benannte Alternative** für jeden Artikel.
- **ITDA-S in Österreich als verantwortlicher EU-Partner** — erreichbar und haftend.
- **Integration und Inbetriebnahme vor Ort durch QmiSoft**, dazu langfristige Ersatzteilversorgung und Verfolgung von Updates.

Kontakt: info@itda-s.com · www.itda-s.com/de/eu-ready/

Quellen und Hinweis

- Verordnung (EU) 2024/2847 (Cyberresilienz-Verordnung): <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>
- Europäische Kommission — CRA Meldepflichten: <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>
- Delegierte Verordnung (EU) 2022/30 (RED-Cybersicherheit): https://eur-lex.europa.eu/eli/reg_del/2022/30/oj
- Europäische Kommission — Funkanlagenrichtlinie (inkl. Aufhebung durch (EU) 2026/339): https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en
- Verordnung (EU) 2023/988 (GPSR): <https://eur-lex.europa.eu/eli/reg/2023/988/oj>
- Verordnung (EU) 2023/2854 (Data Act): <https://eur-lex.europa.eu/eli/reg/2023/2854/oj>
- Verordnung (EU) 2023/1542 (Batterien): <https://eur-lex.europa.eu/eli/reg/2023/1542/oj>
- NISG 2026, BGBl. I Nr. 94/2025: <https://www.ris.bka.gv.at/eli/bgbl/I/2025/94>
- Richtlinie (EU) 2024/2853 (Produkthaftung): <https://eur-lex.europa.eu/eli/dir/2024/2853/oj>
- Verordnung (EU) 2023/1230 (Maschinen): <https://eur-lex.europa.eu/eli/reg/2023/1230/oj>
- Aktueller Stand aller Regeln mit Prüfdatum: <https://www.itda-s.com/de/radar/>

Dieser Leitfaden fasst EU- und österreichische Regeln mit Stand Oktober 2026 zur Orientierung in eigenen Worten zusammen. Er ist keine Rechtsberatung. Verbindlich sind nur die im Amtsblatt der EU und im österreichischen Bundesgesetzblatt veröffentlichten Texte. Termine und Anforderungen können sich ändern; die Industrie hat etwa eine Verschiebung der Cybersicherheitsbestimmungen

der Maschinenverordnung gefordert. Prüfen Sie vor Entscheidungen die aktuellen Rechtstexte oder holen Sie rechtlichen Rat ein.