

EU Rules for Connected Products and Industrial Parts

Why compliance is now mandatory — a guide for buyers, importers and operators (as of October 2026)

ITDA-S — a QmiSoft company · www.itda-s.com

October 2026

Why this matters now

Between December 2024 and January 2027 the European Union is putting a new set of product rules into force. Together they change one thing fundamentally: **whoever places a product on the EU market is responsible for its safety, its cybersecurity and its documentation — for years after delivery.**

For anyone who buys electronics, sensors, automation parts or connected devices outside the EU, this means:

- **The importer carries manufacturer-like duties.** If you buy directly from a factory in Asia and bring the product into the EU, you are the importer — with your own legal obligations.
- **Cybersecurity is now part of product compliance.** A connected device that cannot be updated, has default passwords or no vulnerability handling can be non-compliant, even if it works perfectly.
- **Documentation must exist before the goods are placed on the market** — and must be kept for up to 10 years.
- **Authorities can stop products.** Market surveillance and customs can block, withdraw or recall non-compliant products. Fines under the Cyber Resilience Act reach up to €15 million or 2.5 % of worldwide annual turnover for the most serious breaches.

The rules at a glance

Rule	Applies since / from	Affects	Core obligation
General Product Safety Regulation (GPSR), (EU) 2023/988	13 Dec 2024	All consumer products	An economic operator established in the EU, product identification, safety documentation, incident reporting
Radio Equipment Directive — cybersecurity, Delegated Reg. (EU) 2022/30 (harmonised standards EN 18031)	1 Aug 2025 (until 11 Dec 2027, then covered by the CRA)	Internet-connected radio equipment (Wi-Fi, cellular, Bluetooth, LoRa ...)	Network protection, protection of personal data, protection against fraud

Rule	Applies since / from	Affects	Core obligation
Batteries Regulation (EU) 2023/1542 — producer responsibility	18 Aug 2025	Batteries, also built into devices	Producer registration in each member state, labelling, take-back
Data Act (EU) 2023/2854	12 Sep 2025; design duty for products placed on the market after 12 Sep 2026	Connected products and related services	Inform users about the data a product generates; give users access to their data
Cyber Resilience Act (CRA), (EU) 2024/2847	Conformity bodies 11 Jun 2026 · reporting 11 Sep 2026 · full application 11 Dec 2027	Almost all products with digital elements (hardware and software)	Secure by design, vulnerability handling, security updates for the support period, CE marking, reporting of exploited vulnerabilities within 24 h / 72 h
Austrian NIS2 law (NISG 2026)	In force since 1 Oct 2026; registration by 31 Dec 2026	Larger companies (from 50 staff or €10 m) in 18 sectors	Risk management, incident reporting, supply-chain security — passed on to suppliers
New Product Liability Directive (EU) 2024/2853	National law by 9 Dec 2026	All products incl. software	Strict liability also for software and missing security updates; importers liable when the manufacturer is outside the EU
Machinery Regulation (EU) 2023/1230	20 Jan 2027	Machinery and related products	Replaces the Machinery Directive; protection against corruption (cybersecurity) of safety functions, digital instructions

Also relevant for imports: WEEE / Austrian Elektroaltgeräteverordnung (producer registration in EDM), RoHS, packaging licences, EU dual-use export controls and sanctions screening.

Focus: the Cyber Resilience Act

The CRA is the first horizontal EU law that makes cybersecurity a condition for selling any product with digital elements — from a smart sensor to a PLC with network interface to the software that runs on it.

What manufacturers must do:

1. Assess cybersecurity risks and design the product to be secure (no known exploitable vulnerabilities, secure default configuration, protection of data, minimal attack surface).
2. Handle vulnerabilities: a contact point for reports, a software bill of materials (SBOM), free security updates during the support period (normally at least five years).

3. Document everything in a technical file and an EU declaration of conformity; affix the CE marking.
4. Since 11 September 2026: report actively exploited vulnerabilities and severe incidents — early warning within 24 hours, notification within 72 hours.

What importers and distributors must do:

- **Importers** may only place products on the market whose manufacturer has met the requirements: conformity assessment done, technical documentation available, CE marking affixed, contact details and support period stated. They must add their own name and address, keep documentation available for authorities and inform the manufacturer of vulnerabilities they become aware of.
- **Distributors** check the CE marking, the information supplied and the support period — and must not sell products they know to be non-compliant.
- **Whoever substantially modifies a product** or sells it under their own name or trademark is considered the manufacturer.

Product classes: most products allow self-assessment. “Important” products (class I and II, e.g. routers, microcontrollers with security functions, firewalls) may need third-party assessment; “critical” products may require European cybersecurity certification once a delegated act requires it.

What this means in practice

If you ...	then you must ...
import connected devices or components from Asia	act as importer: check documentation, CE marking, EN 18031 / CRA status, keep records for 10 years
integrate parts into a machine or installation	ensure the whole system is compliant — from 2027 including cybersecurity under the Machinery Regulation
operate installations as a larger company (NIS2)	demand security evidence and update commitments from your suppliers
sell connected products	inform buyers about the data the product generates (Data Act)
keep installations running for 10+ years	plan spare parts, security updates and alternatives from the start

Checklist before you buy a connected part:

- ☐ Who is the manufacturer and who is the EU economic operator?
- ☐ EU declaration of conformity and test reports available?
- ☐ RED / EN 18031 status for radio modules?
- ☐ Defined support period and update policy (CRA)?
- ☐ SBOM and a contact for vulnerability reports?
- ☐ Data Act information on generated data?
- ☐ Export control classification, battery and WEEE registration clarified?
- ☐ Alternative product in case of discontinuation?

How ITDA-S helps — EU-Ready by ITDA-S

ITDA-S takes the whole chain for parts from Asia and Europe: **Source** → **Make EU-Ready** → **Integrate** → **Sustain**.

- **EU-Ready File per article:** datasheet, declaration of conformity, test reports, RED / EN 18031 and CRA status, economic operator.
- **Risk level and a named alternative** for every article.
- **ITDA-S in Austria as accountable EU partner** — reachable and liable.
- **Integration and commissioning on site by QmiSoft**, plus long-term spare parts and update tracking.

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

Sources and disclaimer

- Regulation (EU) 2024/2847 (Cyber Resilience Act): <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>
- European Commission — CRA reporting obligations: <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>
- Delegated Regulation (EU) 2022/30 (RED cybersecurity): https://eur-lex.europa.eu/eli/reg_del/2022/30/oj
- European Commission — Radio Equipment Directive (incl. repeal by (EU) 2026/339): https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en
- Regulation (EU) 2023/988 (GPSR): <https://eur-lex.europa.eu/eli/reg/2023/988/oj>
- Regulation (EU) 2023/2854 (Data Act): <https://eur-lex.europa.eu/eli/reg/2023/2854/oj>
- Regulation (EU) 2023/1542 (Batteries): <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>
- Directive (EU) 2024/2853 (product liability): <https://eur-lex.europa.eu/eli/dir/2024/2853/oj>
- Regulation (EU) 2023/1230 (Machinery): <https://eur-lex.europa.eu/eli/reg/2023/1230/oj>
- Current status of all rules, with dates of last check: <https://www.itda-s.com/radar/>

This guide summarises EU and Austrian rules as of October 2026 in our own words for orientation. It is not legal advice. Only the texts published in the Official Journal of the EU and the Austrian Federal Law Gazette are authentic. Dates and requirements may change; industry has, for example, asked for a postponement of the cybersecurity provisions of the Machinery Regulation. Check the current legal texts or seek legal advice before decisions.