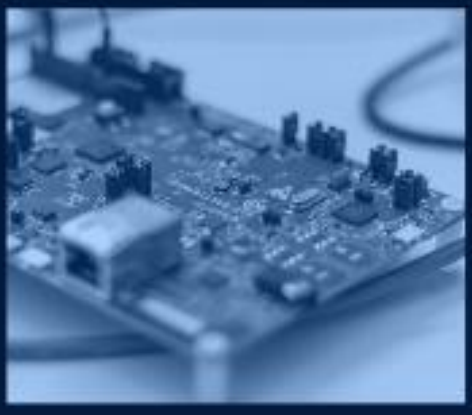
RED-DA

Why compliance is critical for connected devices - now, not later


Vention Technologies B.V
High Tech Campus 27
Eindhoven
The Netherlands

www.vention.nl
info@vention.nl
+31 40 369 0052

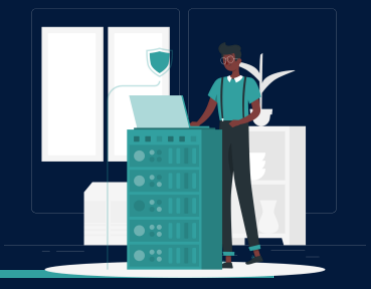
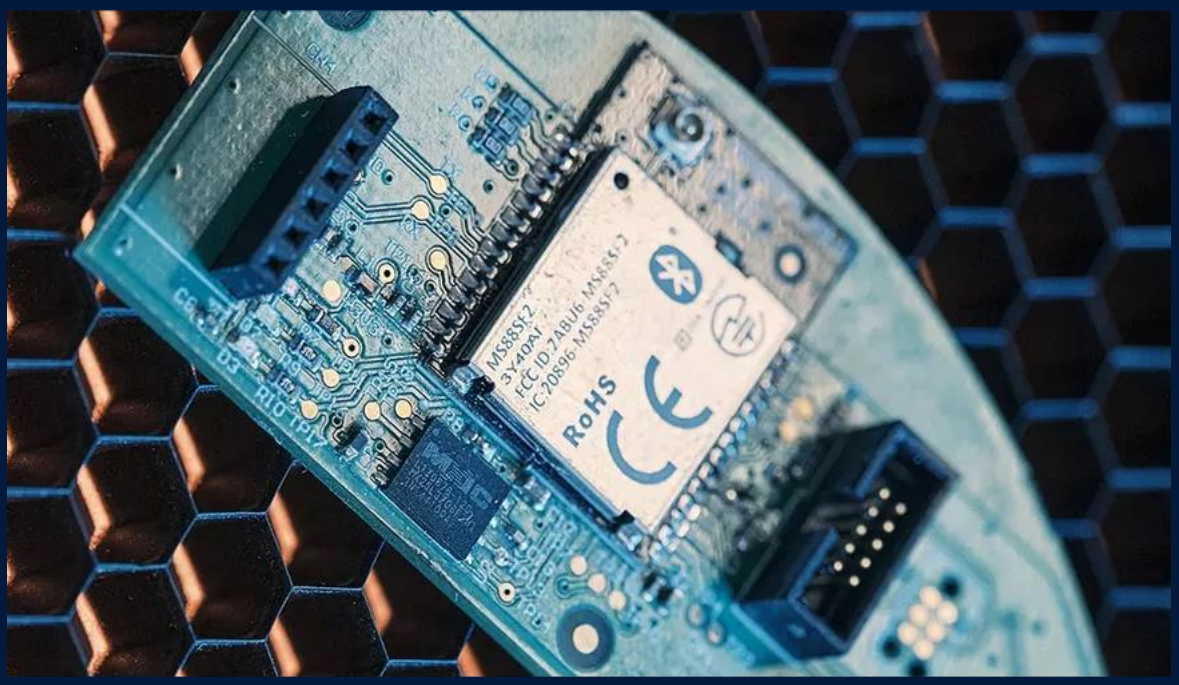


Table of Contents



What is changing and why it matters now

Starting 1 August 2025, most wireless connected devices sold on the EU market must comply with new cybersecurity requirements. These rules were introduced through the RED Delegated Act (EU) 2022/30 and apply to:

- New product introductions
- Existing products sold to the market after 01 August 2025

If your product connects via Wi-Fi, Bluetooth, LTE, LoRa, or other radio channel, it is in scope.

Until now, connected products could legally be shipped with minimum security. From August 1st, 2025, that is no longer the case. Products not complying with RED-DA regulations will be blocked at customs, refused by retailers, or pulled from the market by regulators.

Business risk

Non-compliance is not just failing a test, it:

- Blocks product shipment to the EU market
- Delays the launch of your new product
- Forces redesigns or recalls
- Jeopardizes retail or distribution agreements
- Exposes your brand to security liabilities

Commercial impact

Early compliance protects your budget, timeline, and reputation.

Scenario	Cost impact	Business outcome
Planned from the start	Modest	Smooth RED-DA compliance process, launch on time
Fixed late	High	Redesign, retesting, missed deadlines
Ignored	⚠ Very High	Blocked product shipments, fines, contract loss, liability lawsuits

As the market becomes more aware, customers require RED-DA compliance evidence before issuing a purchase order.

vention

What is required of your product?

RED-DA focuses on three cybersecurity goals:

Clause	Risk	What your product must do
3.3 (d) – Protect network	Devices causing outages or data misuse	Interfaces must be hardened and abuse prevented
3.3 (e) – Protect data	Data leaks, fines, brand damage	Personal data must be encrypted and access must be controlled
3.3 (f) – Prevent fraud	Cloning, overbilling, counterfeit components	Identities and updates must be secure and verifiable

The EN 18031 is the harmonised standard that provides practical guidelines to implement controls to comply with RED-DA.

What to do now?

Use this checklist to spot RED-DA gaps without going through EN 18031. Bear in mind, you need evidence to back up your documentation. Based on the number of gaps, you have a first insight into the amount of work to be done.

#	Cyber-security controls
1	**Secure boot** – device only starts trusted firmware
2	**Signed firmware updates** – OTA or wired
3	**Unique device credentials** – no shared or default passwords
4	**Closed unused network ports** – services inventory complete
5	**Encrypted data in transit** – TLS or equivalent on every interface
6	**Encrypted data at rest** – keys and personal data protected
7	**Personal-data erase on request** – user can request wipe
8	**Event logging & rate-limiting** – protects network resources
9	**Vulnerability monitoring process** – CVE watch and disclosure channel
10	**Software Bill of Materials (SBOM)** – kept with hash values
11	**Technical Documentation index** – every EN 18031 mechanism cross-referenced
12	**Described in manual** – All interfaces and network services are described
13	**EU Declaration of Conformity** – cites RED 2014/53/EU + EN 18031

Need help? Reach out to us and talk to an expert.

Schedule Intro Meeting

How Vention helps

At Vention, we help companies turn connected device ideas into reality and make sure those products meet regulatory, technical, and commercial requirements from day one.

We combine hardware, embedded software, cloud, and compliance expertise under one roof. That means we can guide your product from gap analysis to CE marking and beyond.

What we offer:

1. **Gap analysis**
   Structured quick-scan of your product, mapped to EN 1803. In case product changes are required an assessment is made to determine if an upgrade or redesign is required.
2. **Define roadmap to comply to RED-DA**
   Define an approach and cost estimation to ensure product compliance.
3. **Wockel® approach for new products**
   Our Wockel® development modules are RED-DA ready and form the basis for the development of smart and connected devices.
4. **Compliance filing**
   Complete Technical Documentation and hands-on support with labs and notified bodies.
5. **Support services**
   We provide managed services for connected devices by monitoring vulnerabilities and handling OTA patches.

Regulatory context

From RED to RED-DA

The Radio Equipment Directive (RED) 2014/53/EU has governed safety, EMC and spectrum use since 2016. Article 3(3) has always reserved room for "additional essential requirements"; Delegated Regulation (RED-DA) 2022/30 activates three of them:

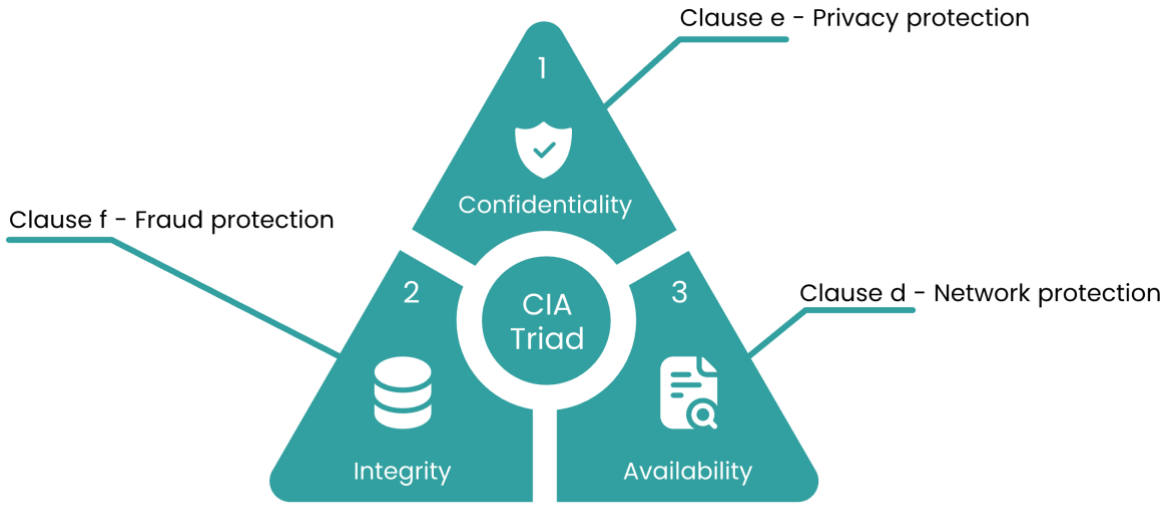
- **3.3 (d)** - the device must not harm the network or misuse resources
- **3.3 (e)** - personal data and privacy of users must be safeguarded
- **3.3 (f)** - the device must resist fraudulent use

The Commission chose a delegated act rather than a full directive revision, meaning the core RED text remains unchanged while the new clauses become directly applicable law after a 30-month grace period. That grace period ends 1 August 2025.

Harmonized standard EN 18031

To give manufacturers a presumption of conformity, the standardization bodies drafted EN 18031-1 (internet-connected radio equipment), EN 18031-2 (personal data-processing radio equipment such as wearables, toys and childcare devices) and EN 18031-3 (devices concerning economic value exchange). Each standard maps concrete security mechanisms (e.g. authenticated firmware update, interface hardening, best-practice cryptography) to the three legal clauses and specifies what evidence the technical file must contain.

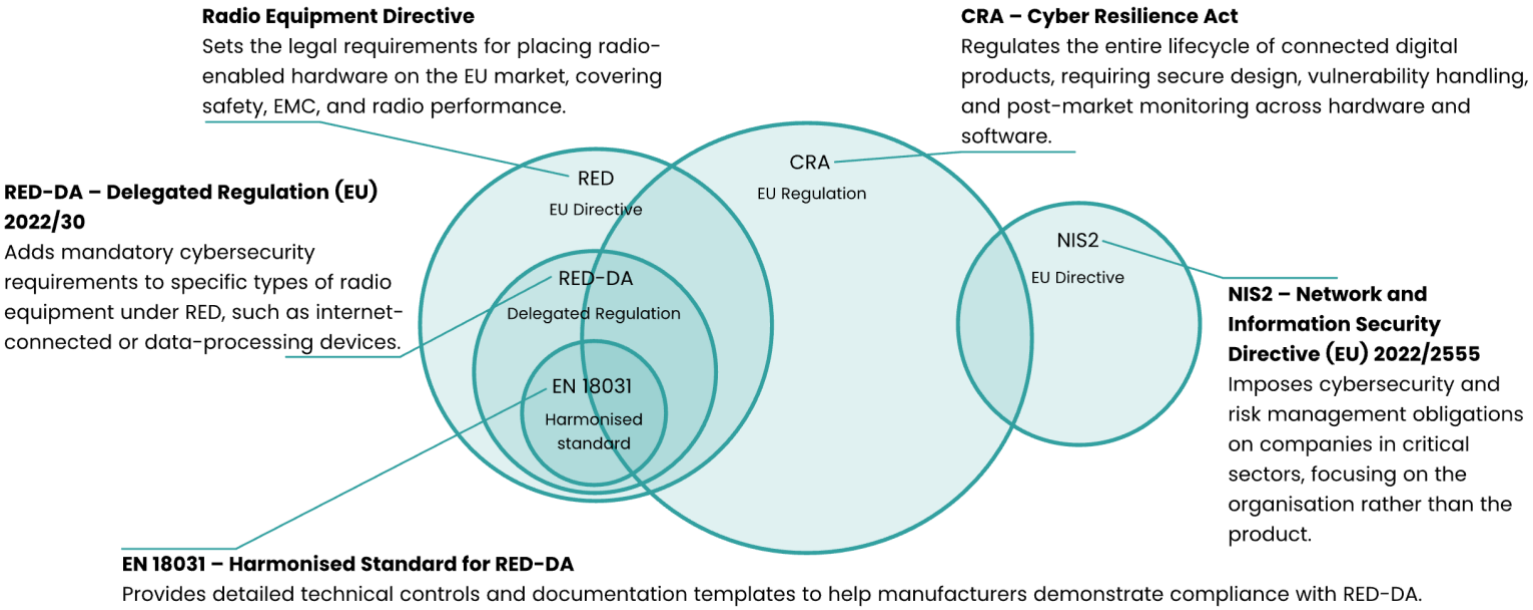
Focus areas of the clauses in relation to the security-triad



Simplified view. All clauses touch all CIA elements to some extent.

How RED-DA interacts with other EU files

- **Cyber Resilience Act (CRA)** - broader in scope: covers the entire digital product, including cloud services. Full compliance is mandatory on 11 December 2027. RED-DA focuses only on the radio product itself.
- **NIS2 Directive** - targets the operator's organisational security posture. For device makers NIS2 chiefly adds incident-reporting obligations once products are in service.
- **RED** - frame the overall conformity-assessment logic (self-assessment vs notified body, technical documentation layout).



Products that fall under RED-DA

The Delegated Act cover most electronic gadget with a radio. Its scope catches most connected devices that reach the EU market.

What's in scope?

A product is in scope when it contains (a) a "radio" interface as defined in RED Article 2, and (b) at least one interface able to communicate autonomously via the internet or with other radio gear. Classic examples are Wi-Fi thermostats, BLE wearables, LoRa sensors, LTE-M asset trackers, NFC payment readers and GNSS-enabled drones. In contrast, a wired-only industrial PLC or a passive RFID tag remains outside RED-DA.

Scope decision flow

1. Does it connect to the internet directly or through a gateway? → **EN 18031 Part 1** applies
2. Does it connect to another radio equipped device that allows for indirect internet connectivity? → **EN 18031 Part 1** applies
3. Does it process personal, traffic or location data? → **EN 18031 Part 2** applies
4. Does it handle payment transactions? → **EN 18031 Part 3** applies

What's most affected?

Smart home and energy	Personal health and sport	Industrial sensing and tracking
PV inverters EV chargers Smart plugs Energy management systems	Personal wearables GPS watches Fitness trackers Cycling power meters Patient home monitoring systems	LoRaWAN or LTE-M nodes LTE trackers and field sensors Smart pumps Industrial vibration sensors

Essential cybersecurity requirements

Once a product is confirmed in scope, three short clauses in the RED become the engineering target.

Clause	Objective	Typical attacks blocked
3.3 (d)	Do not harm the network or misuse its resources	Botnets, DDoS attacks
3.3 (e)	Safeguard users' personal data and privacy	Eavesdropping, data scraping, unauthorized telemetry
3.3 (f)	Protect users against fraud	Firmware tampering, counterfeit peripherals, replay attacks

EN 18031 translates these into mechanism families such as secure update mechanisms, access-control mechanisms and secure storage mechanisms.

Network protection – clause (d)

The standard demands rate-limiting, secure boot and hardening of exposed services. A 2024 outage at a Dutch ISP traced back to thousands of insecure GNSS trackers illustrates the business risk: the operator throttled all tracker SIMs, creating a wave of field returns. Building basic firewall rules and exponential back-off into the firmware would have prevented it.

Privacy protection – clause (e)

Wearables that upload heart-rate data must encrypt data in transit and at rest, implement local data-wipe on user request, and expose a privacy dashboard. A large toy maker had to withdraw a smart doll in 2023 because voice logs were left unencrypted on cloud storage. The recall cost exceeded the full original R&D budget - proof that privacy design is cheaper than crisis PR.

Fraud protection – clause (f)

Secure element–backed device identity and signed peripheral authentication stop counterfeit battery packs or sensor cartridges. In 2025 an e-scooter brand lost €2M to cloned chargers that overbilled the backend. Simple HMAC-based mutual authentication would have blocked the clones at handshake time.

Harmonised standard EN 18031

EN 18031 turns the three RED-DA clauses into a checklist of security mechanisms that can be objectively tested. The series has three parts: Part 1: internet-connected radio equipment, Part 2: personal data and part 3: payment data. A product can fall under one or more parts, depending on its interfaces and data assets.

Mechanism families

Each family bundles related controls, for example:

Abbrev.	Purpose	Typical controls
ACM	Access control	RBAC, DAC, MAC options
AUM	Authentication	Password strength, brute-force protection
SUM	Secure updates	Signed or channel-protected firmware delivery
SSM	Secure storage	Confidentiality and integrity of keys and data
RLM / NMM / TCM	Resilience and monitoring	Rate-limiting, logging, traffic shaping
CRY	Cryptography	Best-practice algorithms and key lengths

Part 2 adds privacy-focused families such as LGM (logging), DLM (deletion) and UNM (user notification) that build on Part 1 requirements.

Applicability and appropriateness flow

For every mechanism the standard first asks *Is it needed?* then *Is the chosen implementation strong enough?* Applicability and appropriateness are recorded in a structured template with three verdicts: PASS, FAIL, NOT APPLICABLE.

Documenting for RED-DA compliancy

RED-DA expects security to be planned at concept stage, not bolted on at the end. Good documentation is therefore as critical as good code.

Threat modelling and risk assessment

Start with assets, interfaces and actors, then map the threats. EN 18031 Annex A explains how threat modelling drives the applicability of each mechanism. Record risks, mitigations and residual exposure.

Security architecture description

Provide:

- block diagram with trust boundaries,
- list of external interfaces matched to mechanism families,
- data-flow table noting encryption, authentication and storage method.

Mark each element with the internal references used in the technical file so reviewers can trace requirements quickly.

Evidence sets

EN 18031 prescribes unique identifiers:

- *E.Info.* – descriptive information,
- *E.Just.* – justification of decision-tree paths,
- *DT.* – decision tree nodes.

Using these tags inside document filenames or section headers lets auditors auto-cross-reference evidence.

Lifecycle considerations

Document processes for:

- vulnerability monitoring and coordinated disclosure,
- signed over-the-air updates with rollback protection,
- secure decommissioning or data wipe at end-of-life.

With these artefacts in place you will spend review meetings discussing substance rather than searching for missing files – a direct cost saver as lab day-rates rise ahead of the 2025 deadline.

Assessment

Build the technical documentation (TD) dossier

The dossier must be ready before the start of assessment. A practical TD table of content is:

1. Product description and bill of materials
2. Radio interface overview with spectra and power levels
3. Risk assessment and threat model (cross-referenced to Blue Guide/RED Guide)
4. Mapping of RED Art. 3 (3)(d)(e)(f) to EN 18031 mechanism families
5. Evidence sets: schematics, source references, test reports, vulnerability scans
6. Copy of user information and privacy notices
7. Draft DoC

Choose the assessment route

- Module A (Internal production control). Allowed when the product fully applies harmonised standard EN 18031 and the security risks are low to medium.
- Module B+C or H (Notified Body involvement). Recommended for high-risk use cases (for example payment terminals) or when the design deviates from EN 18031.

The assessor uses three test angles:

1. **Conceptual** – check the rationale and evidence.
2. **Functional completeness** – verify that all interfaces and assets are covered, often with network scanners.
3. **Functional sufficiency** – test the strength, e.g. fuzzing an interface or tampering with an update flow.

Decision trees guide these checks and require the manufacturer to justify each path, making the process repeatable and transparent.

Reference list

European Commission. (2022). *Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU with regard to the application of the essential requirements referred to in Article 3(3)(d), (e) and (f). Official Journal of the European Union*, L 6, 1–14.

European Commission. (2025). *Commission Implementing Decision (EU) 2025/138 of 28 January 2025 on the harmonised standards for radio equipment drafted in support of Directive 2014/53/EU. Official Journal of the European Union*, L 138.

European Parliament and Council. (2014). *Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment (Radio Equipment Directive). Official Journal of the European Union*, L 153, 62–106.

NEN - EN 18031-1:2024. *Common security requirements for radio equipment – Part 1: Internet-connected radio equipment.* (2024). European Committee for Standardization (CEN) and European Committee for Electrotechnical Standardization (CENELEC).

NEN - EN 18031-2:2024. *Common security requirements for radio equipment – Part 2: Internet-connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment.* (2024). CEN and CENELEC.

Disclaimer: This whitepaper has been prepared with care to provide guidance and insights. However, it may not account for the specifics of your individual situation and should not be regarded as exhaustive or definitive advice.