What the RED Delegated Act means for end-products using Nordic Semiconductor components

---

Disclaimer

---

1. What is the RED Delegated Act?

The RED Delegated Act (EU) 2022/30, under the **Radio Equipment Directive (2014/53/EU)**, is an extension focusing on **strengthening cybersecurity** requirements for wireless and internet-connected devices in the European market.

It activates **three essential requirements (Articles 3.3 (d), (e), (f))** that mandate:

- Protection of networks from harm or misuse – Article 3.3(d)
- Protection of personal data and user privacy – Article 3.3(e)
- Protection against fraud and unauthorized monetary transactions – Article 3.3(f)

Enforcement Date: **1 August 2025.** As of this date, products put on the EU market shall comply with the RED Delegated Act. Even if a product line was sold before, **new batches after 1 August 2025 must comply** regardless of earlier compliance status (see also Blue Guide sections 2.2 and 2.3).

The RED Delegated Act is expected to be replaced by the **Cyber Resilience Act (EU)** in 2027.

---

2. Does RED apply to my product?

The Delegated Act applies to specific **types of radio equipment**, particularly when they meet certain functional thresholds:

Requirement	Applies if...
3.3(d) - Network Protection	The device is **Internet-connected** (directly or indirectly, e.g. via a smartphone app)

3.3(e) - Privacy Protection	The device **processes personal data, traffic data, or location data** — or is a **toy, wearable, or childcare product**.
3.3(f) - Fraud Protection	The device **supports monetary transactions** or transfers of value (e.g. digital wallets).

A device may fall under more than one requirement. Nordic is not positioned to assess which requirement applies for a type of application, as it will largely depend on the end-product features.

Examples of products falling under the RED Delegated Act:
Devices capable of communicating via the Internet: smartphones, tablets, electronic cameras; telecommunication equipment as well as equipment that constitutes the 'Internet of Things', connected machinery and industrial IoT.
Toys and childcare equipment: toys with radio function, baby monitors
Wearables: smartwatches, fitness trackers.

---

3. The new Harmonized Standard EN 18031

The **ETSI EN 303 645 Standard** of 2020 was developed for consumer IoT products, but was not deemed suitable for use as a Harmonized Standard for the RED DA. The newly developed and published **EN 18031 Standard** heavily re-use provisions from the EN 303 645 Standard, and is composed of three documents:

EN 18031-1 – Protection of the network (3.3(d))

EN 18031-2 – Personal data and privacy (3.3(e))

EN 18031-3 – Protection from financial fraud (3.3(f))

Unfortunately, the EU Commission had some reservations with the EN 18031 standard and only recognized it as Harmonized Standard '**with Restrictions**'. This means that one cannot currently use EN 18031 for a 'presumption of conformity' (i.e. if a product complies with all the standards requirements, one could presume conformity). As the EU Commission needed to apply restrictions, each manufacturer must **assess its product's compliance with the listed restrictions** to determine whether self-declaration is possible or if the conformity assessment must be conducted by a Notified Body and additional risk assessment is required. Risk assessment will help determine whether certain requirements can be bypassed based on the intended use of the product or whether compliance remains mandatory.

The results of a **SESIP** evaluation of connected/IoT platforms on which radio equipment are based can be used as evidence to support compliance (EN 18031 – Annex D).

The EN 18031 series recommends the implementation of a Secure Development Lifecycle which would aid in the ability to satisfy the security requirements:

- Clarifying Security Objectives, which could be done through a Security Target document
- Implementing Security by Design processes
- Performing Threat Modelling
  Following NIST Cybersecurity best practices such as NISTIR 8259, NIST SP 800-series, FIPS 140-2/3

---

4. How to demonstrate compliance with the RED Delegated Act?

End-product manufacturers must demonstrate and show compliance with the RED Delegated Act and other applicable regulations in order to apply the **CE-marking** and sell products in the EU. The regulations are supported by detailed Standards which set out several requirements. The **EN 18031 Standard** (of Q1/2025) was developed especially for the RED Delegated Act.

To demonstrate compliance manufacturers shall:

- Establish technical documentation.
- Affix the CE-marking.
- Produce an EU Declaration of Conformity.
- Maintain documentation at the disposal of national authorities for 10 years after the product was placed on the market.

End-product manufacturers have two options to show compliance:

1: Self-Declaration (Annex II)

- Allowed when harmonized standards are used **without restrictions**, and in case of restrictions, provided the restriction does not apply to the specific end-product.
- Supported by **EN 18031 series** (covering network protection, privacy, and fraud prevention).

2: Third-Party Assessment (Annex III)

- Manufacturers can work with a **Notified Body** to undergo an independent evaluation and receive CE-marking.
- Required if:
  - Harmonized standards are **not used**, or
  - Standards **with restrictions** are **used**, and such restrictions apply to the end-product.

Restrictions noted for EN 18031 can change quickly, but currently (2025-05-26) include areas like:

- The sections ‘rationale’ and ‘guidance’
- Use of default passwords

- Parental controls
- Payment security handling

---

5. How Nordic's PSA Framework supports your compliance journey

As a **semiconductor manufacturer**, Nordic is actively supporting its customers through:

Modular Compliance via PSA Certified

- Nordic is working with **PSA Certified** and a **Notified Body** to assess if **PSA Level 1 requirements** are considered acceptable to demonstrate compliance with several RED provisions and how customers could leverage Nordic's certificates to help **fast track their demonstration of compliance** for their end-products when using Nordic reference designs.
- You can find the PSA and SESIP certificates on our security landing page

Secure Design Lifecycle

- Nordic's design approach (following the PSA Framework) ensures that key security concepts are integrated, such as **Secure-by-Design and Security in Depth**, and that writing **Security Target**, security objective and Threat Modelling are performed.
- You can learn more about Nordic's security features in our Nordic platform security whitepaper

Control of the Supply Chain

- Nordic has a **Product Security Incident Response Team (PSIRT)** in place since 2020.
- Nordic runs a **bug bounty** program on the 'Yes We Hack' platform.
- Provides customers with tools like **Software Bill of Materials (SBOM)** generation for traceability.
- Maintain a portal for receiving and reporting security vulnerabilities Security Advisories & Disclosure Portal.

---

6. How does RED relate to other Cybersecurity Regulations

In the EU:

- **PSTI Act (UK)**: Similar scope as RED and recognizes RED compliance (effective as of 29 April 2024).
- **RED Delegated Act**: Radio equipment (wireless products). Focus on the security of the end-product (effective as of 1 August 2025).

- **Cyber Resilience Act (CRA)**: Broader scope, covering all digital products across their lifecycle including software products, emphasizing security-by-design and vulnerability management and reporting; compliance begins **Q2027** (Q4 2026 for security updates). Standards developed for the RED Delegated Act are expected to be used also for CRA.

In the US:

- **FCC Cyber Trust Mark** (voluntary IoT labeling started May 2024).
- **NIST-aligned standards** apply to public sector device procurement.

Nordic's frameworks (e.g. NIST SP 800-series) ensure cross-border security compatibility.

---

7. Failure to comply with the RED Delegated Act

Possible consequences of non-compliance with RED Delegated Act include:

- **Financial penalties**, which vary widely between countries.
- **Market Access Denial:** Products not complying cannot be legally placed on the EU market and Customs authorities may detain or reject shipments at the border, and distributors and retailers may refuse to sell or stock such products.
- **Contractual liabilities**: Indemnities granted to distributors and retailers.

---

8. Recommended Next Steps

Recommendation:

1. **Classify your product**: Determine which of your wireless products are in scope.
2. **Choose a conformity path**: Self-declare or work with a Notified Body.
3. **Use harmonized standards**: Start with the EN 18031 series (though meeting ETSI EN 303 645 may very well be sufficient for certain products).
4. **Integrate Cybersecurity in Product Development**: Ensure compliance with the RED Delegated Act and the soon-in-force CRA from the design phase.
    - Implement secure-by-design principles
    - Document all cybersecurity decisions and testing
5. **Document your compliance**:
    - Perform a cybersecurity risk assessment
    - Technical file, providing detailed information on how the product complies with Article 3(3) (d) – (f), including evidence such as test reports, audit logs, and software update mechanisms
    - EU Declaration of Conformity
    - CE marking

6. **Engage Nordic**:
    - Leverage PSA Certified platforms and documentation
    - Use SBOM and security advisories
    - Coordinate on shared certification efforts

---

8. Revision history

Version 1 (28/05/2025)

1. First version of RED Customer guide

Annex A

Extract from RED Delegated Act (EU) 2022/30:

Article 3(3), point (d) – Network protection

It enhances network protection by requiring devices to have features that prevent harm to communication networks and avoid disrupting the functionality of websites or services.

- *shall apply to any radio equipment capable itself to communicate over the internet, regardless if it communicates directly or via any other equipment ('internet-connected radio equipment') i.e., such internet-connected equipment operates protocols necessary to exchange data with the internet either directly or by means of an intermediate equipment.*

Article 3(3), point (e) – Personal data and Privacy protection

It strengthens the protection of personal data and privacy. This includes measures to prevent unauthorized access or transmission of consumers' personal data.

- *shall apply to any of the following radio equipment, if that radio equipment is capable of processing, within the meaning of Article 4(2) of Regulation (EU) 2016/679, personal data, as defined in Article 4(1) of Regulation (EU) 2016/679, or traffic data and location data, as defined in Article 2, points (b) and (c), of Directive 2002/58/EC:*

  (a) internet-connected radio equipment, other than the equipment referred to in points (b), (c) or (d);
  (b) radio equipment designed or intended exclusively for childcare, such as child monitors.
  (c) radio equipment covered by Directive 2009/48/EC (toy with radio function);
  (d) radio equipment designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung from any of the following (wearable radio equipment'):
    - *any part of the human body, including the head, neck, trunk, arms, hands, legs and feet;*
    - *any clothing, including headwear, hand wear and footwear, which is worn by human beings; such as radio equipment in the form of wrist watch, ring, wristband, headset, earphone or glasses.*

(12) Additionally, as regards the protection of personal data and privacy, radio equipment for childcare, toys with radio function and wearable radio equipment pose security risks even in the absence of an internet connection. Personal data can be intercepted when radio equipment emits or receive radio waves and lack safeguards that ensure personal data and privacy protection. This equipment can monitor and register a number of the user's sensitive (personal) data over time and retransmit them through communication technologies that might be insecure. Protection of personal data and privacy should be ensured, when the equipment is capable of processing of personal data, or traffic data and location data Article 3(3), point (e), of Directive 2014/53/EU should therefore apply to that radio equipment.

Article 3(3), point (f) – Protection from fraud

It aims to reduce the risk of fraud, mandating features like improved user authentication controls to minimize fraudulent electronic payments and monetary transfers.

- *shall apply to any internet-connected radio equipment, if that equipment enables the holder or user to transfer money, monetary value or virtual currency as defined in Article 2, point (d), of Directive (EU) 2019/713.*