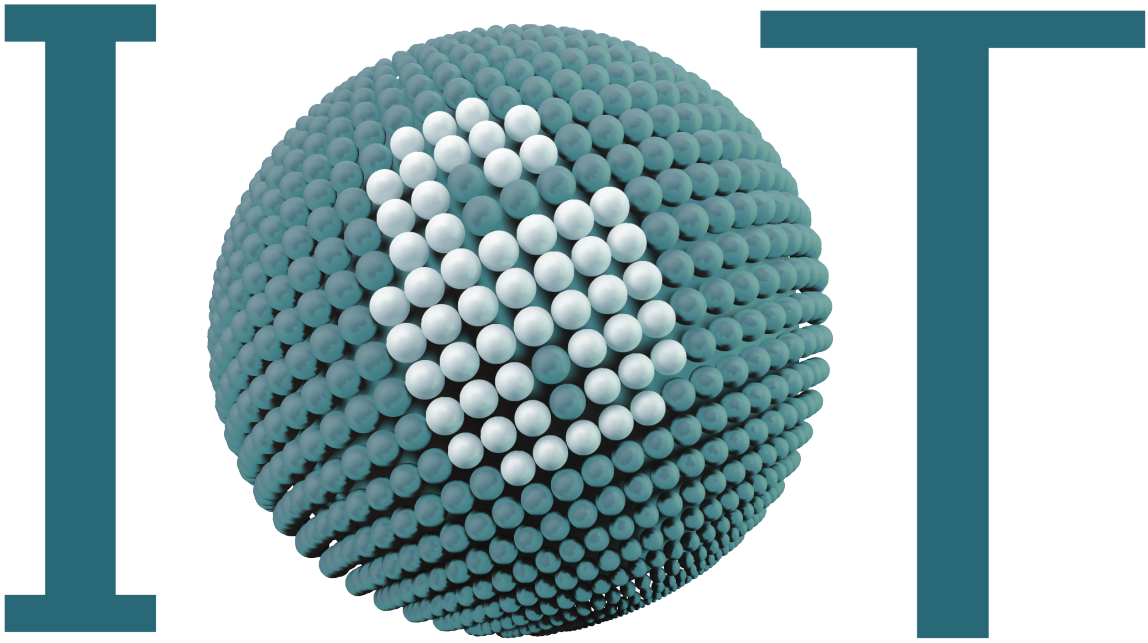

Security Foundation

EUROPEAN UNION RADIO EQUIPMENT DIRECTIVE (EU RED) EXECUTIVE BRIEF

An IoTSF Regulatory Watch group publication

Radio Equipment Directive Delegated Act (EU) 2022/30			
Official Source	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0030		
Geographic Region	European Union	affected industries	cross-industry
Scope	Internet-connected radio equipment and wearable radio equipment		
In brief	1. radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service 2. radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected 3. radio equipment supports certain features ensuring protection from fraud		
Consequences	Non-compliance with the Directive may result in products being prohibited from sale in the EU market, enforcement actions by regulatory authorities, and potential financial and reputational damage to the manufacturer.		
Baseline Standard	EN 18031-1:2024 EN 18031-2:2024 EN 18031-3:2024		

The European Commission (EC) has advanced efforts to enhance cybersecurity for Internet-connected radio equipment within the EU by implementing a delegated act under the Radio Equipment Directive (RED). While initially set for enforcement in August 2024, the regulation's start date has been extended to 1st August 2025, to allow time for the development of harmonized standards. Beginning on this date, in-scope wireless devices and products sold in the EU must comply with the requirements set by the RED Delegated Act (EU) 2022/30. Throughout this document, the Radio Equipment Directive as modified by Delegated Regulation (EU) 2022/30 will be referenced as "RED DA"

To provide guidance on implementing cybersecurity measures for radio equipment, ensuring devices meet essential RED DA requirements for network security, data privacy, and fraud protection as defined in Articles 3(3)(d), (e), and (f) of the EU's Radio Equipment Directive, the EN 18031 standard was developed by the European Committee for Standardisation (CEN) and European Committee for Electrotechnical Standardisation (CENELEC) and adopted by the European Union on 30th January 2025.

The EN18031 standard is structured into three parts, each addressing different aspects of cybersecurity for Internet-connected radio equipment:

1. **EN18031-1:2024**: Covers general security requirements for radio equipment, addressing network security risks.
2. **EN18031-2:2024**: Focuses on data and privacy protections for devices handling personal or sensitive data, including IoT devices like wearables and toys.
3. **EN18031-3:2024**: Pertains to devices handling virtual or monetary values, focusing on fraud protection.

It is important to note that the three parts of EN 18031 are not necessarily mutually exclusive. Depending on the functionality and risk profile of a device, one or more parts may apply in parallel. It is therefore important to understand the risk profile of your device and determine which sections impact you.

The EN 18031 standard includes decision trees and pass/fail criteria to help manufacturers evaluate product compliance and mitigate vulnerabilities effectively. The standards are set to become mandatory from 1st August 2025, aligning with RED DA's deferred cybersecurity enforcement date.

1. Does RED DA apply to me?

The Radio Equipment Directive (RED) delegated act on cybersecurity ("RED DA") will apply to you if you manufacture, import, or sell internet-connectable radio equipment in the European Union.

Specifically, the delegated act applies to:

- Most radio equipment that is directly or indirectly connectable to the Internet, such as IoT devices, industrial machinery, consumer electronics, and other equipment with a radio interface. This encompasses any electrical or electronic product capable of Internet communication, either directly or through intermediary devices. This broad scope reflects the growing reality that even devices not traditionally seen as 'Internet-connected' - for example, those communicating via Bluetooth, Zigbee, or proprietary wireless protocols - could still form part of Internet-connected systems when paired with gateways, smartphones, or networked controllers. Therefore, such equipment falls under the same baseline cybersecurity expectations as devices with native Internet access using the Internet Protocol (IP) as transmission protocol. Despite differing interpretations, with some stakeholders arguing that only devices communicating via IP should be considered 'Internet-connected', the prevailing

regulatory intent focuses on functional connectivity (i.e. capability of the device as opposed to design intent) rather than protocol specificity.
- Non-internet-connectable radio equipment used in toys, childcare products, and wearables that process personal or location data.
- Internet-connected radio equipment that enables monetary transactions.

The following sectors are specifically excluded from articles 3.3 e) and f) (EU) 2022/30:

- Devices intended for type approved motor vehicles (EU 2019/2144)
- Devices for medical use (EU 2017/745)
- Devices for Civil Aviation (EU 2018/1139)
- Devices for Road Toll systems (EU 2019/520)

It's important to realize that these sectors still need to conform with 3.3 d).

2. What do I have to do to achieve and maintain compliance with RED DA?

There are three main things you need to do for each product that you intend to bring to market on or after 1st August 2025:

1. Determine whether it falls within the scope of the act;
2. If so, ensure that it meets the RED DA requirements that apply to it;
3. Provide the necessary evidence to demonstrate that it meets the requirements.

The three essential requirements that are brought into effect by the recent enactment of RED DA address the following topics:

a. In-scope radio equipment must not adversely affect the network it is attached to/is part of.
b. Where relevant, it must include safeguards to protect the personal data (which is not limited to data actively provided by the user, such as an individual login, but also includes data passively collected by the device, such as location information or usage patterns) as well as privacy of the user and subscriber; see Article 4, point (1), of Regulation (EU) 2016/679
c. Radio equipment that enables transfer of money, monetary value, or virtual currency must support features ensuring protection from fraud.

As a first step, you should determine whether the product under consideration falls within the scope of one or more of these requirements. The Networking and Fraud requirements are aimed only at internet-connected equipment, but the Privacy requirement extends also to childcare equipment, toys with radio functions, and wearable devices, even if not internet-connected. Medical devices are explicitly excluded from scope of all three requirements as they are already covered by provisions of existing regulations, while vehicles and their components, aviation equipment and electronic road toll systems are within the scope of (3.3 d)), but not (3.3 e) and f)).

In the case of a product that is already close to market, you should assess to what extent it already meets the relevant requirements, note the areas of non-conformity, and plan how to address them. To ensure that future products meet the requirements, you would be wise to update design and development processes to build compliance in from the ground up.

A series of harmonised standards has recently been published to help organisations ensure that their products address these essential requirements. EN 18031-1, -2 and -3 respectively cover the network, privacy, and fraud requirements, and following the ones relevant to your product should make achieving compliance easier. Adherence to harmonised standards generally implies a 'presumption of conformity' with associated EU regulations, i.e. if you prove you have applied the standard correctly, then it is assumed your product complies with the regulation. In the case of RED and EN 18031-1, -2 and -3, however, there are certain restrictions qualifying this presumption concerning the ability of users to set passwords, and of parents and guardians to control access. These standards and restrictions are discussed in more detail in section 6, below.

The RED DA provides for three alternative conformity assessment procedures, the simplest of which involves self-declaration based on assessment of conformity to the relevant harmonised standards. These procedures are also discussed in section 6, below. In all cases, you are expected to provide technical documentation including design information, evidence in support of conformity assessment methods used, copy of the declaration of conformity, and test reports.

3. How does the RED DA interact with the CRA?

RED DA and the CRA are closely linked in intent, with the CRA effectively set to supersede the cybersecurity requirements of the RED DA. According to Article 69 (Transitional Provisions) of the CRA, CE marks that have been applied under the RED DA will remain valid until six months after the CRA becomes applicable (11th December 2027), which is currently expected to be 11th June 2028. After this period, the CRA will take full effect as the primary legislative instrument governing cybersecurity for products with digital elements placed on the EU market.

Organisations currently preparing for RED DA compliance should view this as an opportunity to lay the groundwork for CRA readiness. The CRA has a broader scope - covering all products with digital elements, not just radio-connected devices - and introduces new obligations including risk assessments, reporting of security incidents, and stricter vulnerability handling requirements. Nonetheless, RED DA compliance is a stepping stone, not a detour. Processes and controls developed for RED DA can be reused or extended for CRA conformance.

4. How do I do it?

Manufacturers of in-scope products must ensure compliance to product-relevant **Essential Requirements** as specified in Article 3 of RED Delegated Act. Therefore, manufacturers need to conduct comprehensive risk assessment in order to identify product-relevant Essential Requirements while assessing and addressing cybersecurity vulnerabilities within their product.

Manufacturers need to identify and select appropriate standards for ensuring compliance to these product-relevant RED DA requirements and perform conformity assessment as per Annex II of RED DA. In most cases CENELEC EN 18031 standards series can be used as a basis of meeting RED DA based on the presumption of conformity embodied in the harmonised standard. But, be aware that additional restrictions exist in the adopted act in the EU Official Journal, which differ from EN18031 and must be adhered to. It is also possible to follow a standard such as EN303645 as a means to meet RED DA. However, in this case, since EN303645 is minus a presumption of conformity then guidance from a notified body should be sought to support the decision to use a different route.

In addition, manufacturers need to develop thorough technical documentation in accordance with RED (Annex II, III or IV), in order to demonstrate compliance with relevant RED DA requirements.

Lastly, before placing a product on the market, a Declaration of Conformity (DoC) must be provided by the manufacturer according to the requirements in Annex VI of RED. A self assessment-based DoC can be done by the manufacturer if a “harmonized” standard is used (e.g. CENELEC EN 18031), alternatively the manufacturer can produce a DoC in cooperation with a recognized testing body (Notified Body).

5. What happens if I don’t do it?

In short you will be unable to legally CE mark your product and place it on the market in the EU.

a. Since this is a CE compliance requirement then, without the updates and assessment to meet the cyber amendments your product will be non-compliant to RED DA so you will be unable to place your product on the EU market.
b. Whilst you may already have a product, which is compliant from a radio emissions and susceptibility perspective. The updates to the original RED regulations, sections 3.3 d), e) ,f) relate to Cyber Security and infer a substantial change to the product which results in a requirement to re-certify.
c. Penalties for non-compliance do exist and may come in the form of fines, withdrawal of non-compliant products from the market, seizure of non-compliant products and reputational damage. Penalties vary across the EU member states. A consideration here however revolves around the RED certificates expiring around mid-2028 nominally 6 months after the CRA enters enforcement. Since the RED DA will effectively be absorbed into CRA it is logical that the penalties imposed by CRA would apply to radio products previously covered under RED.
d. For reference, ‘placing on the market and ‘making available on the market’, are explained in sections 2.2 and 2.3 of the EU Blue Guide which discusses the implementation of EU product rules (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_247_R_0001). Of note here is that a product can be placed on the market only once and placement refers to an individual item, not a type a series. This is important to understand since this, along with the substantial modifications

required to the product to implement the cyber amendments, requires a product to be compliant with regulations at the time it is placed on the market. To this end, products of a type currently on the market and in use with end customers met the requirements on the date they were placed on the market. New versions of the same type of product, updated to meet the cyber amendments, when they are placed on the market must meet the regulations in place at that time. The fact that you already have products of the same type in the market has no assumed inheritance when placing 'new' products on the market.

Failure to re-certify and re-test the product for the cyber security amendments would result in a non-compliance of the product, which results in an inability to place the product on the market.

6. How do I demonstrate conformance to the requirements?

To demonstrate conformance to the requirements of the RED DA, manufacturers may ensure that their radio equipment meets the cybersecurity provisions introduced by the harmonized standard series EN18031. Manufacturers are free to demonstrate conformance by other means but will likely lose the possibility of self-declaration. Depending on the type of radio equipment, EN18031 details the cybersecurity requirements for the device - note that multiple standards may apply to a given device:

1. **EN18031-1:2024**: Covers general security requirements for internet-connected radio equipment, addressing network security risks.
2. **EN18031-2:2024**: Focuses on data and privacy protections for devices handling personal or sensitive data, including IoT devices like wearables and toys (whether or not internet-connected) .
3. **EN18031-3:2024**: Pertains to devices handling virtual or monetary values, focusing on fraud protection.

It is important to be aware of the differences between the EN18031 standard and the requirements for the presumption of conformity based on commision implementing decision 2025/138 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500138).

One note of importance is that the implementing decision requires that passwords are used in all sections -1, -2 and -3 whereas in the EN18031 standard it is allowable for no passwords to be implemented in -1 and -2. Additionally the implementing decision finds that the standard is insufficient in incorporating parental access controls (in -2), and in the provisions for secure updating of financial systems (in-3) Full details can be found in the official document linked.

Following one of the above harmonized standards, the following options are available to conduct conformity assessments in alignment with the radio equipment directive (**Directive 2014/53/EU** / https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053) :

A. Internal Production Control (Annex II)
   The manufacturer ensures that the product meets the essential requirements through internal design and production controls.

A self-declaration of conformity is issued, and technical documentation is maintained.
No third-party assessment is required.

B. EU-Type Examination + Internal Production Control (Annex III)
   A Notified Body assesses a sample of the product to confirm compliance with the essential requirements.
   Once approved, the manufacturer ensures ongoing compliance through internal production controls.
   A Declaration of Conformity is issued based on the Notified Body's approval.
C. Conformity Based on Full Quality Assurance (Annex IV)
   The manufacturer implements a quality management system that covers product design, manufacturing, final inspection, and testing.
   A Notified Body audits the quality assurance system and issues a certificate of conformity.
   The manufacturer must maintain ongoing compliance with quality assurance procedures.

Manufacturers must also ensure that their technical documentation includes cybersecurity risk assessments, mitigations, and testing results. Compliance with harmonized standards provides a presumption of conformity, simplifying the assessment process.

7. Where do I start?

As mentioned above, as a first step, it is important to have an overview of the current assets and products that are currently on the European market or planned to be placed on the European market. Divide them into assets for which RED DA applies and assets that are only relevant later for the CRA. For each product under RED DA either planned, under development, or still shipping to distributors or direct to customers, consider the following:

A. Products already shipping, or under development and close to release to manufacture:

1. Is the product within scope of RED DA? Refer to Section 1 of this document.
2. If the product does not comply with the requirements of RED DA, it cannot receive a CE mark and therefore may not be placed on the European Market. Thus, stop CE Marking and shipping to the EU.
3. Perform Risk Assessment/Gap Analysis vs EN18031, while considering CRA provisions in parallel.
4. Create a remediation plan. Consider whether it is more cost effective to implement RED DA compliance (required immediately) / CRA compliance (required December 2027) sequentially or in parallel.
5. Perform remediation, following the procedure in 6 above (for RED DA conformance), culminating in Declaration of Conformity, CE Marking and then resume/begin shipping to EU

B. Products in planning or early development

RED DA applies from 1st August 2025 to 11th December 2027 after which CRA applies and is (broadly) a superset of RED DA requirements. CE Marks obtained under RED DA will remain valid until 11th June 2028. OEMs must balance the benefits of time-to-market with the potential costs of two sequential compliance projects, complicated by the absence of a harmonized standard to codify a presumption of conformity to CRA, not likely to appear until 2026. Attention must also be paid to CRA Reporting obligations of manufacturers (Article 14) that come into force earlier already on 11th September 2026. Processes for RED DA should be designed with this in mind and considered as a first mile-stone to becoming CRA compliant.

Therefore the key question, taking this into account is: should a product under development be looking to conform to EN18031, given that RED DA will be superseded by the CRA in the near future?

1. Is the product within scope of RED DA?
2. Perform Risk Assessment, and plan/continue development according to requirements of CRA. Ensure additional requirements of EN18031 -1, -2, and -3 are included if in scope. Conformity to future harmonized standards (in respect of CRA) should be planned, using EN 18031 as a guide for overlapping elements of CRA until draft standards for CRA are published. RED DA provisions will not apply from June 2028.
3. If not in scope, proceed with best practice towards CRA compliance by December 2027.

The IoTSF publishes the IoTSF Security Assurance Framework (IoTSF-SAF) as a practical guide which aims to help product manufacturers follow a 'Secure by Design, Secure by Default' method throughout the product lifecycle. The requirements are published at https://af.iotsf.org/ with a supporting Security Assurance Questionnaire available to members. Within the latest release V4.0, the questionnaire also provides a mapping for EN18031 to the IoTSF-SAF.

Additional, valuable information can be found on:

- Main website - https://iotsecurityfoundation.org/
- Best Practice Guides and Whitepapers https://iotsecurityfoundation.org/best-practice-guidelines/
- IoTSF Security Assurance Framework - https://af.iotsf.org/