FAQs about Radio Equipment Directive (RED) Cybersecurity Requirements

The EU Commission published a delegated regulation to the Radio Equipment Directive (RED), with the aim to improve the cybersecurity of wireless products on the European market. These new requirements will be mandatory from 1 August 2025.

What is the RED?
The Radio Equipment Directive (RED) is a European Directive which regulates the placing of radio equipment on the EU market.

It sets out essential requirements and conformity assessment procedures that manufacturers and importers of radio equipment must adhere to before placing their products on the EU market.

The existing RED essential requirements, radio performance, safety and electromagnetic compatibility (EMC), have recently been extended by a delegated regulation requiring cybersecurity compliance for certain products.

What do the RED cybersecurity requirements mean?
The RED cybersecurity requirement aims to increase the level of cybersecurity, personal data protection and privacy, and protection of financial transactions through the activation of Articles 3.3 (d), (e) and (f) as essential requirements:

- Article 3.3 (d) - radio equipment does not harm the network or its functioning, nor misuse network resources, thus causing an unacceptable degradation of service.
- Article 3.3 (e) - radio equipment includes safeguards to protect the personal data and privacy of the user and the subscriber.
- Article 3.3 (f) - radio equipment supports certain features ensuring protection from fraud.

Which typical devices are covered by the RED cybersecurity requirements?

1. Equipment that uses radio technology for communication over the internet such as mobile phones, tablets, and telecommunication equipment
2. IoT devices that can transmit data over the internet
3. Toys and childcare equipment such as baby monitors
4. Wearable devices such as smartwatches or fitness trackers
5. Connected industrial devices

What is outside the scope of RED cybersecurity requirements?
The following is completely excluded for RED Article 3.3 (d), (e) and (f):

- Medical devices

The following are excluded for RED Article 3.3 (e) and (f):

- Aviation
- Motor vehicles
- Electronic road toll systems

The following are excluded for RED Article 3.3 (e) and (f):

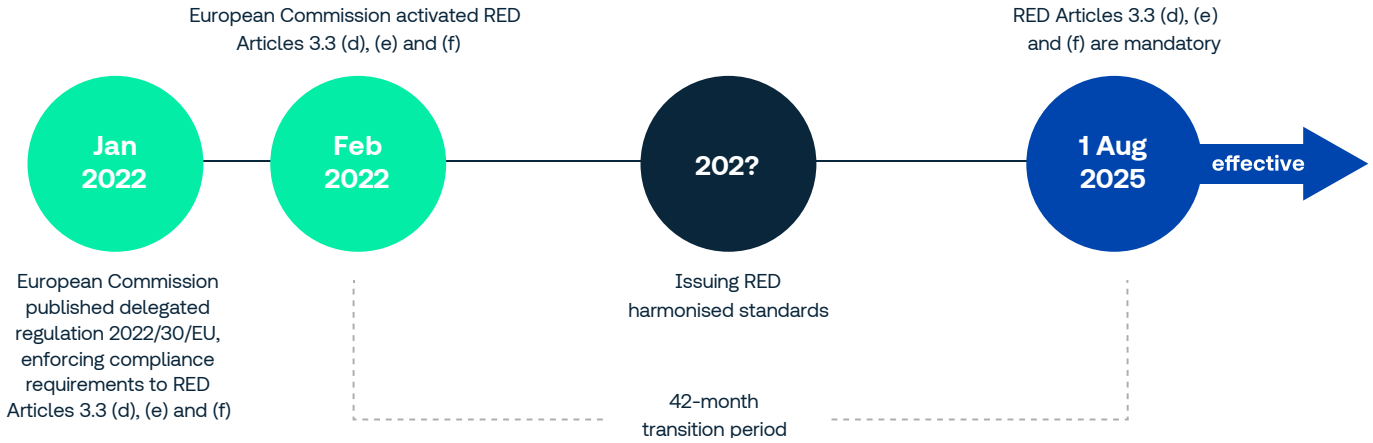
- Radio products that are not connected to the internet, such as a DAB broadcast receiver and radar that are products under the scope of the RED, but are not in the scope of the RED cybersecurity requirements.

What happens to old devices already placed on the EU market?
Devices that do not have specifications for addressing security issues may still be used until the end of their life. Legislation and the RED applies to each individual radio product placed on the market, not a series of products.

Therefore, all individual radio products being placed on the EU market after 1 August 2025 will need to comply with these new cybersecurity requirements.

Are there harmonised standards?
To date, harmonised standards are currently not available, but these are being developed by CEN/CENELEC of which TÜV SÜD is an active member, contributing to this development.

When is the deadline to comply with the RED cybersecurity requirements?
The European Commission has confirmed a 1-year extension of transition period for the Delegated Act (2022/30) to the Radio Equipment Directive (2014/53/EU) aimed at improving the cybersecurity of wireless devices available on the European Union's market. These cybersecurity requirements will be mandatory from 1 August 2025.



TÜV SÜD is an EU Notified Body for the Radio Equipment Directive.

How can TÜV SÜD help?
TÜV SÜD provides testing and evaluation services based on standards such as EN 303 645 and IEC 62443. Our laboratories can perform a variety of tests and services to prepare for the incoming regulation. We are also actively involved with the development of cybersecurity standards globally.

In addition, TÜV SÜD is an EU Notified Body for the Radio Equipment Directive. Therefore, we can support you in complying with the requirements of the Radio Equipment Directive together with other regulations and standards applicable to radio equipment and devices.

- Understanding if your radio equipment product is in the scope of RED cybersecurity
- What are the best practices presently, such as secure-by-design
- Understanding the present status of standardisation
- How to plan to ensure confidence in the security of your product

What manufacturers should do now?
While the extended period will allow more preparation time for manufacturers, the transition timeline should not result in a delay in preparing and assessing the cybersecurity health of their products.

Manufacturers of wireless products are advised to consult with TÜV SÜD early in the product development process to plan the necessary steps and start evaluating their products now instead of waiting for the standards to be published. It is key to engage in advanced preparation and early actions.

Contact TÜV SÜD today to understand how we can help prepare for the incoming RED cybersecurity requirements. We can also further assist in increasing security for your products.

Related services

TÜV SÜD provides the following related services
- IoT security spot check
- IoT penetration testing
- TÜV SÜD Cybersecurity Certified (CSC) certification
- Test according to standards and AoC (EN 303 645 and NIST IR 8259)
- Security training for consumer IoT stakeholders

TÜV SÜD AG Westendstr. 199, 80686 Munich, Germany
+49 89 5791-0 cps@tuvsud.com www.tuvsud.com/cps