

Radio Equipment Directive

What is the Radio Equipment Directive (RED)?

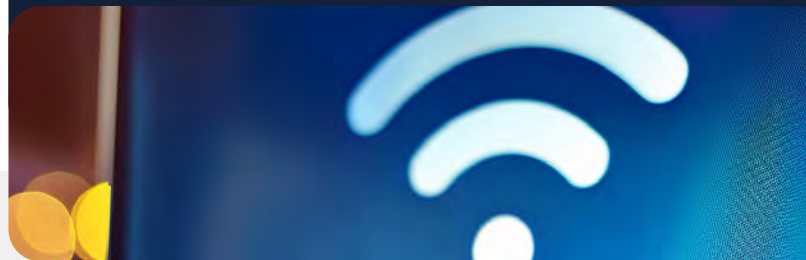
The EU Directive 2014/53/EU defines the requirements for radio equipment and wireless devices placed on the European Union market. Its goal is to ensure security, efficiency, and the harmonized use of the radio spectrum.

What is covered by the RED?

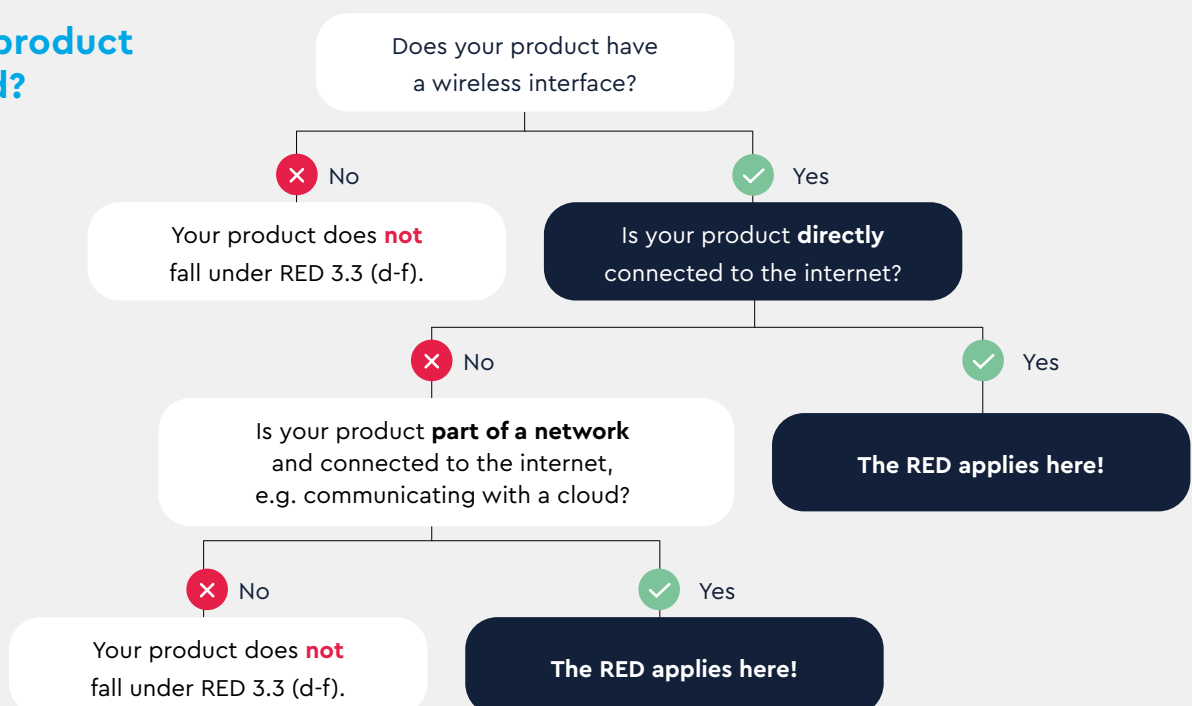
- Communication devices (mobile phones, radios)
- IoT & smart devices (wearables, IoT sensors)
- Does your product have a wireless interface?

What is new?

Since August 1, 2025, the technical specification for radio equipment (EN 18031) have come into effect. This specification clarifies Article 3 of the RED and defines cybersecurity requirements. All products covered by the RED and placed on the EU market must comply with these additional security standards to obtain the coveted CE marking. This regulation is the EU's response to the increasing threat of cyberattacks on connected devices with wireless interfaces.



Is your product affected?



Is your product covered by the RED? We'll guide you. The Cybersecurity Requirements at a glance

Article 3.3 (d)

Protection of Networks

Radio equipment must not have harmful effects on networks or their operation. This is to prevent, among other things, that a radio device or its functions are misused to damage a network.

Article 3.3 (e)

Protection of Personal Data

Radio devices must provide adequate security measures to protect personal data. This applies, for example, to a smartwatch that processes health data and is connected to the internet.

Article 3.3 (f)

Protection against Fraud

Radio devices must have features that protect against fraudulent activities or manipulation. For example, the payment function on a smartphone must have dedicated security measures.



EN 18031

This standard specifies the RED cybersecurity requirements for your product.

What security mechanisms are defined in the standard, and how does your product comply with them?

- Access control
- Authentication
- Secure updates

- Secure storage
- Secure communication
- Resilience

- Cryptography
- Network monitoring
- General device properties

WE THINK ONE STEP AHEAD.

**Expert advice. Comprehensive service.
Highest quality.**

Is your product facing its market launch?

We'll guide you through meeting all necessary standards.

Do you have a product idea that may fall under the RED regulations?

With the help of our ethical hackers, we'll develop your product securely and CE-compliant – Secure by Design.



Your partner for Cybersecurity

TQ-PCC Augsburg

Our DAKKS-accredited Product Compliance Center tests your product according to international standards in compliance with EN ISO/IEC 17025. Fast, cost-efficient, and customer-oriented.



Ralf Wagner

Cybersecurity Specialist & Manager

+49 371 33151-36

ralf.wagner@tq-group.com

