FAQ – Radio Equipment Directive (RED) Cybersecurity Requirements

New connectivity technologies and concepts drive the industry up to a forcast of 29 billion connected devices by 2022. Therefore, the European Commission has taken action to improve the cybersecurity of wireless devices on the European market. In October 2021 new RED requirements were published on the EU's official website.

WHAT HAS CHANGED?

The Delegated Regulation complements the EU Radio Equipment Directive RED 2014/53/EU by activating article 3(3)(d), (e) and (f). The target is to increase the level of cybersecurity, personal data protection and privacy for certain categories of radio equipment.

3 SECTIONS OF ARTICLE 3.3 SPECIFIC TO CYBERSECURITY

(d) Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.

(e) Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.

(f) Radio equipment supports certain features ensuring protection from fraud.

www.tuv.com/wireless

TÜVRheinland®
Precisely Right.

RED CYBERSECURITY REQUIREMENTS – TRANSITION PROVISIONS

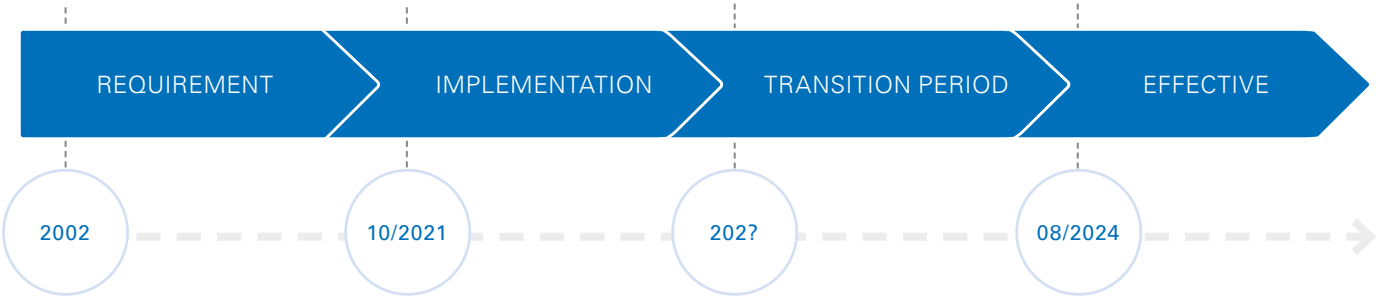
- (EU) 2016/679 GPPR 2002/58/EC
- (EU) 2019/881
- (EU) 2019/713
- (EU) 2016/1148
- (EU) 910 (2014)

RED 3 (3) (d), (e), (f)

- Self assessment, when product design follows harmonized standards
- Rely on third-party assessment (CEN/CENELEC)

Issuing RED Harmonized standard

Requirements are mandatory



WHEN WILL IT BE EFFECTIVE?

The new cybersecurity requirements were published in October 2021, and came into force in February 2022 with a transition of 30 months. It shall apply from Aug. 1st, 2024. That means we expect the issuing of a harmonized standard in the beginning of 2023. Unless a harmonized standard is available, you have two options to achieve compliance:

1. Perform a self-assessment to show your product has been designed in accordance with state-of-the-art-standards and practices.
2. Perform a third-party assessment by an independent inspection body like TÜV Rheinland, regardless of whether or not a (harmonized) standard was used. TÜV Rheinland is working on a RED compliant requirement catalogue (2PfG standard) which will cover the various areas (Authentication / Interface security / Communication security / Software update / Privacy protection / Transaction security).

Manufacturers who wait for the harmonized standard will have only a transition period of approximately 10-12 months before the changes become mandatory in August 2024.

We prove the quality of your products
to ensure integrity and performance.
Speak with an expert today!

ONLINE CONTACT

TÜV Rheinland
Corporate Headquarters
Cologne, Germany
+49 221 806-0
wirelessIoT@tuv.com
www.tuv.com/wireless

WHICH PRODUCTS WILL BE AFFECTED?

1. Devices capable of communicating via the internet (e.g. Smart phones, tablets, electronic cameras, telecommunication equipment, IoT devices)
2. Toys and childcare equipment (e.g. baby monitors, toys)
3. Smart wearables (e.g. Smart watches, fitness trackers)

YOUR RELIABLE PARTNER

As a Notified Body in the EU to the Radio Equiment Directive (RED), we support you all over the world to protect your products to the highest possible standards as well as providing professional evaluation according to ETSI EN 303 645.

- Faster Product Launch
- Easy access to new markets
- Worldwide testing laboratories
- Simplified and convenient application process
- Full service from planning to market launch
- Interdisciplinary work with product and certification experts

VALUE ADDED SERVICES

- R&D support services
- Pretesting
- Service offering together with preferred partners for services (e.g. GCF, PTCRB)
- Fully automated test systems solutions
- Any other electrical regulatory testing services

TÜVRheinland®
Precisely Right.