Ready, RED, Go?

Requirements under the Radio Equipment Directive for internet-connected devices starting August 1, 2025

07 July 2025

On August 1, 2025, additional cybersecurity requirements will come into force for a large number of electronic devices under the Radio Equipment Directive (Directive 2014/53/EU; RED). Despite this approaching deadline, many issues are still unclear, in particular the scope of application of the new regulations and the interpretation of the term "internet-connected radio equipment ".

Overview of the RED

The RED lays down certain product safety standards for radio equipment. Radio equipment includes all devices that can emit or receive radio waves for communication or location purposes. In addition to the classic radio, this includes all devices connected with wireless internet or Bluetooth capabilities, i.e. cell phones, notebooks, WiFi routers, GPS trackers, etc. Most of these product requirements have been in force since June 13, 2017 and therefore apply to all devices placed on the market after this date. In Germany, the Radio Equipment Act (Funkanlagengesetz or FuAG) serves to implement the RED.

Many other requirements have been subsequently added, including for common charging capabilities, which came into force on 28 December 2024.

New requirements for radio equipment connected to the internet

For some regulations, the European Commission must define certain product categories to be covered by the regulation, such as Art. 3 (3) RED. Art. 3 (3) (d-f) RED sets out technical requirements with regard to network security, data protection and fraud protection, which are specified in detail by European standardization organizations such as the European Committee for Standardization (CEN).

With the Delegated Regulation 2022/30/EU, the Commission has now "activated" Art. 3 (3) (d-f) RED. CEN has developed the harmonized standards EN 18031-1 for network security requirements, 18031-2 for data protection and EN-18031-3 for fraud protection. The technical requirements of EN 18031-1 include mechanisms for access control, authentication, secure communication and network monitoring.

Scope of Art. 3 (3) (d-f) RED

However, these new standards are not applicable to all radio equipment within the

meaning of the RED. Rather, they only apply to radio equipment that can itself communicate via the internet, regardless of whether it communicates directly or via other devices ("internet-connected radio equipment"). Without a doubt, this refers to all devices that can receive or send data directly via the Internet, i.e. smartphones, laptops and various smart home devices.

It should be noted that the device in question does not necessarily have to be connected to the internet via radio waves. Devices that can send or receive certain data via radio waves but are only connected to the Internet via cable are also included. This primarily includes WiFi routers.

A more difficult question is the extent to which devices that are not directly connected to the internet but can only send and receive data to and from the internet via other devices are also included. These are, for example, devices that exchange data with internet-capable devices via Bluetooth, such as wireless cameras, microphones, sensors, etc. Industry representatives have been advocating to only include as internet-connected radio equipment those wireless devices that can also execute internet-capable protocols themselves. This interpretation would expressly exclude Bluetooth devices. The responsible authorities (including the Federal Network Agency or Bundesnetzagentur in Germany) have not yet provided a clear line, nor has the European Commission, which offers basic interpretation aids in its RED Guide.

In addition, the data protection requirements under Article 3(3)(e) RED also apply to radio equipment used for childcare (so-called baby monitors), toys within the meaning of Directive 2009/48/EC and radio equipment worn on the body. The latter primarily includes smartwatches.

By contrast, medical devices within the meaning of Regulation 2017/745/EU and in vitro diagnostic medical devices within the meaning of Regulation 2017/746/EU are excluded from the scope of Art. 3 (3) (d-f) RED.

Further EU cybersecurity requirements

When it comes to the cybersecurity of products, not only the requirements of the RED that must be considered. Regulatory overlap is possible with regard to the new Networks and Informations Systems Security Directive (Directive 2022/2555/EU; NIS 2 Directive) or the Cyber Resilience Act (Regulation 2024/2847/EU; CRA).

The NIS 2 Directive sets security requirements for operators of critical infrastructure. Although the transposition deadline for member states expired on October 18, 2024, only nine member states have transposed the directive so far, including Belgium and Italy. While the Netherlands and Austria are expected to implement the directive this year, France, Spain and Germany are likely to implement it much later. The German Federal Ministry of the Interior did not publish a draft bill on the implementation of the NIS 2

Directive until the end of May 2025, which means it is likely to take until next year for the bill to come into effect.

The CRA places certain requirements on products with digital elements with a network connection. The cyber security requirements listed in Annex I Part I include control mechanisms against unauthorized access, data encryption and the monitoring of internal activities. The CRA comes into force on December 11, 2027. As a regulation, it is directly applicable in all member states and does not require implementation on a national level.

In contrast to the RED, the CRA also covers devices without radio capabilities, i.e. devices that only send and receive data by cable. The cybersecurity requirements of both legal acts overlap to a considerable extent. In general, it can be assumed that the CRA requirements are more comprehensive and stricter than those in Art. 3 (3) (d) RED. Some even assume that the CRA will render the RED cybersecurity requirements obsolete.

Conclusion

Despite clear technical standards, there are still unanswered questions regarding the scope of application of the RED, particularly with regard to devices with an indirect internet connection. There are further uncertainties regarding the relation to the NIS 2 Directive and the CRA. It is therefore advisable for manufacturers to take a comprehensive look at the EU cybersecurity requirements already at an early stage. To this end, conscientiously carrying out a conformity assessment procedure in accordance with Art. 17 RED is essential.

BLOMSTEIN will follow further developments and keep you informed. Leonard von Rummel will be happy to answer any questions you may have regarding product regulation and cyber security.

***