February 2024

Radio Equipment Directive

Are you ready for the EU cybersecurity requirements for Radio Equipment and IoT devices?

pwc

www.pwc.com

Introduction

Recent *statistics* predict the number of Internet of Things (IoT) devices worldwide will almost double from **15.1bn** in 2020 to more than **29bn** in 2030. With that in mind, it is not an overstatement to say these devices play a significant role in society and our private lives. As such, the European Commission (EC) updated the Radio Equipment Directive (RED) in February 2022 with a new delegated Regulation (i.e. the Regulation 2022/30/EU) to effectively manage/enforce the cybersecurity requirements of equipment using the radio spectrum, thus, covering most IoT devices.[1]

In particular, the new act imposes stricter requirements on manufacturers on the following elements: Network protection, personal data privacy, as well as protection from monetary fraud for wireless products that can communicate by means of wireless technology, either directly or through other accessory equipment. The new act will be enforced per 01 August 2025[2] and applies to a wide range of organizations involved in the manufacturing, import, and distribution of radio equipment.

1 Most Internet of things (IoT) or connected devices are considered to use radio or wireless technology. For this reason, such devices fall under the scope of RED.
2 Originally scheduled for enforcement in August 2024, the new Regulation has been postponed to 2025 due to ongoing preparation of harmonized standards.

RED's extensive product scope:

The equipment which is put under the lens of the mandatory cybersecurity requirements uses the radio spectrum to intentionally transmit and/or receive radio waves for the purposes of radio communication and/or radiodetermination (either by itself or through another accessory).[3]

This practically means that the product scope of RED is broad and careful consideration is needed whenever assessing if your company's equipment, intended for EU consumers, falls under the RED scope and its applicable requirements.

To be more specific, in this day and age, most devices are equipped with radio based wireless capabilities, meaning that RED covers a broad range of products: from smart TVs, mobile phones, tablets and laptops to wireless toys and children's safety equipment (such as baby monitors) to devices with Wi-Fi, Bluetooth, 5G, GPS or Zigbee capabilities, as well as routers, broadcasting devices (such as Chromecast), wearable devices (such as smartwatches and fitness trackers), radars, etc.

Having said that, there is a list of products which is **exempted** from RED, such as:

- Radio equipment used by radio amateurs,
- Marine equipment,
- Airborne products, parts and appliances (note that consumer drones are in scope),
- Custom-built evaluation kits destined for professionals to be used solely at research and development facilities[4],
- Radio equipment exclusively used for activities concerning public security (such as defence and State security) or for the economic well-being of the State[5], and,
- Wired Telecom Terminal Equipment (TTE).

The new legislative update confers responsibility on product manufacturers, importers and distributors to comply with the RED cybersecurity obligations[6] before placing wireless connected devices/radio equipment on the EU market.[7] What does this mean in practice though? And more specifically, what does this mean in terms of compliance in the absence of formal technical requirements?

3 'Radio equipment' means an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination.
4 See, Annex I of RED in this regard.
5 Article 1(3) of RED.
6 Stipulated under Article 3(3)(d),(e),(f) of RED.
7 'Placing on the market' means the first making available of radio equipment on the EU Union market.

How to prepare for RED?

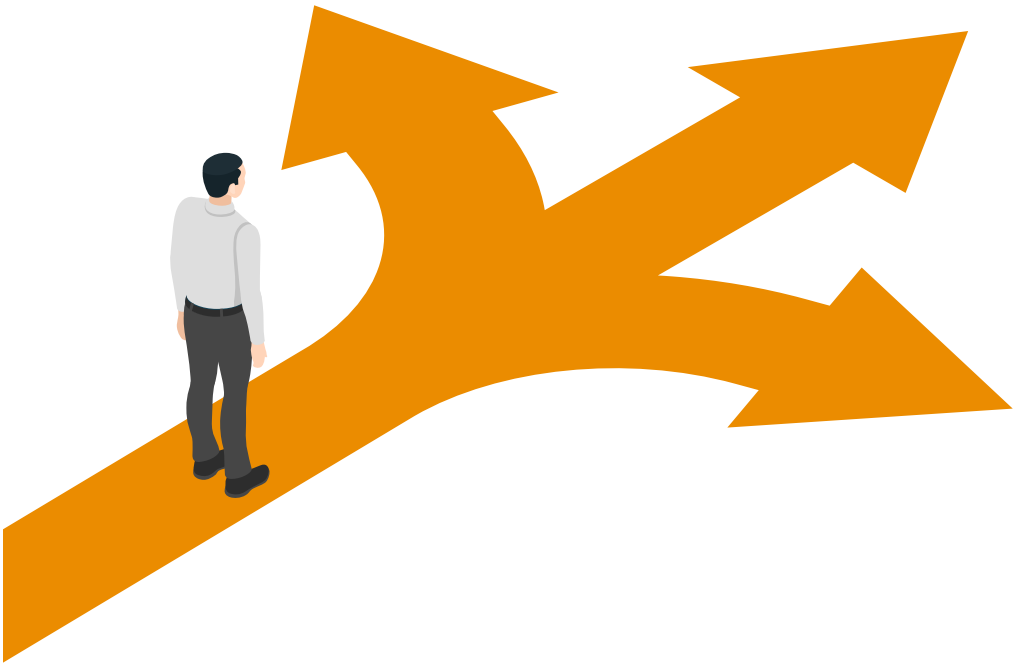
The new Regulation and its mandatory requirements will apply from 1st of August 2025. In order to achieve compliance with the new act, RED provides for the following conformity assessment routes:

1. **Internal production control** (as outlined in Annex II of RED)
2. **Examination by a notified body** (as outlined in Annex III of RED)
3. **Full Quality Assurance** (as outlined in Annex IV of RED)

Route 1 constitutes a self-assessment procedure, where the manufacturer ensures its wireless product meets all essential cybersecurity requirements set out in the new Regulation. To this end, technical documentation and an EU declaration of conformity (DoC) are issued by the respective manufacturer.

Route 2 consists of an audit of the manufacturer's technical documentation and supporting evidence by a Notified Body. The Notified Body will issue an EU-type examination certificate, which guarantees the respective manufacturer complies with the new Regulation and its requirements.

Route 3 equals to a conformity assessment based on full quality assurance – or, put differently, it is a conformity assessment process which combines elements from the 1st Route (i.e. Internal production control) with examination of the respective manufacturer's quality assurance system by a Notified Body.



Harmonized Standards:

For radio equipment manufacturers, RED offers a presumption of conformity with its mandatory cybersecurity requirements, when the wireless equipment is designed and built according to relevant harmonized standards (which can be found *here*).[8]

If harmonized standards are available for a wireless product to prove conformity with the essential requirements, manufacturers are free to choose the conformity assessment route that suits them best. If no harmonized standards are available for their radio equipment – or if the relevant standards are not fully applied – manufacturers need to involve a Notified Body during their assessment procedure (i.e. Routes 2 or 3).

*Please note that if you are a non-EU based manufacturer wishing to sell your wireless products into the EU, you must first demonstrate compliance with the RED mandatory requirements (see **Routes 1,2,3** previously discussed) before applying for **CE marking**.*

8 The applicable harmonized standards contribute to demonstrating compliance with the essential cybersecurity requirements specified in Article 3.3 of RED; they encompass/include technical characteristics for the radio equipment falling under the RED scope.

What should radio equipment manufacturers, importers and distributors do now?

Now is the time to take action. Yet, with so many different requirements and legislation coming up, it is difficult to know where to start and/or how to proceed. We have detected a quick summary of steps for you to take and get started:

1. **Check if your business is affected.** Determine if your product falls within the scope of RED and the forthcoming essential cybersecurity requirements.
2. **Understand the requirements and assess your security baseline.** Often, the requirements are written with a high-level description that does not tell you what actions you should take. This makes it difficult to determine whether you already comply with some requirements or how to implement them in accordance with your business purposes. Thus, it is useful to translate the requirements to practical guidelines and do an assessment of your current security baseline. After that, you can determine where you already comply, and what you should focus on to further improve. From a practical perspective, while implementing the essential cybersecurity requirements, you also need to think of 'user friendliness', 'user experience' and 'societal impact' during the entire lifecycle of your products: Build future proof devices where firmware updates is 'key' in order to ensure your current and future products do not risk becoming obsolete/illegal in the near future. Put differently, devices that are easy to hack, do not include features for better user authentication (access management controls) and/or transport layer security protocols will definitely not meet the essential cybersecurity requirements and have a negative impact for your company, the end-user, as well as the environment and society overall.
3. **Identify the harmonized standards that are applicable to your product/radio equipment**. Review the *EU Official Journal of RED* for updates on the available harmonized standards. It is expected that three new CEN-CENELEC standards will be published by June 30, 2024 covering the essential cybersecurity requirements. Until then, you could, for example, refer to ETSI EN 303 645[9] and IEC 62443[10], which are already published standards that are expected to significantly influence the development of the CEN-CENELEC anticipated harmonized standards.
4. **Educate employees and spread awareness.** Achieving compliance with the new Regulation and its essential requirements will need the involvement of multiple departments and functions/stakeholders across the entire organization. In order to promote the necessary awareness, it is important to communicate and educate affected employees about the new requirements.
5. **Update your Declaration of Conformity (DoC).** Review and update your DoC so it accurately demonstrates all applicable requirements to your wireless equipment. Also, ensure it makes a reference to the harmonized standards used to provide the presumption of conformity.

9 ETSI 303 645 is the first global cybersecurity standard for consumer IoT products, creating a cybersecurity baseline for manufacturers which can help ensure cybersecurity is incorporated into IoT products from their design.

10 The IEC 62443 standard is intended to secure Industrial Automation and Control Systems (IACS).

6. **Keep your technical documentation up to date.** Create a technical file for your product and maintain it for ten (10) years (after the product was placed in the EU market). Review Annex V of RED for further information on what needs to be included in your technical documentation.
7. **Self-declaration / EU type certification.** Self-declare your compliance with the essential requirements, if a harmonized standard is published in the RED Official Journal. Yet, in the absence of harmonized standards, your conformity assessment options are: i. The EU type certificate process (Annex III of RED), or ii. the full quality assurance process (Annex IV of RED).

Use case/example:
The Dutch Government Inspectorate for Digital Infrastructure (RDI) warned in a *study* that solar panel inverters do not meet requirements for cybersecurity, as they can be hacked very easily and / or cause interference to other wireless IoT devices too. Studies have also found that, if successful, an orchestrated attack which can remotely enable and disable a multitude of solar panels, could regrettably bring the Dutch powergrid down.

How can PwC be of help?

PwC is here to help you throughout your cybersecurity journey and regardless of your maturity or development stage. We offer you a suite of cybersecurity services and solutions that can help you meet your expectations: **Testing, scoping tools, risk assessments, conformity assessments / gap analyses, certification and other security and privacy related services** (e.g. Privacy-by-design & Security-by-design assessments, effective implementation strategies, response measures tailored to the needs of your organization, etc.) that can boost your confidence and further increase the cybersecurity posture of your radio equipment / IoT products.

With our multidisciplinary pool of experts, we can also support you with an **EU-type examination** certificate, which will demonstrate compliance with the mandatory cybersecurity requirements stemming from the new Regulation / delegated act.

If you are interested in a **gap assessment to ETSI EN 303 645 and IEC 62443-4-2**[11] standards (which include requirements expected to be overlapping with those from the anticipated CEN-CENELEC harmonized standards[12]), PwC can also help you in this regard and contribute to the enhancement of your cybersecurity resilience throughout the entire lifecycle of your IoT devices.

Remember: The new delegated act[13] is only one of the various EU cybersecurity acts that manufacturers targeting EU consumers need to comply with. By helping you comply with the relevant act, though, we can - at the same time - help you comply with cybersecurity and privacy requirements stemming from other EU mandatory legislation too: e.g. NIS2, CER, CRA, DORA, GDPR, etc.. We are here for you to perform gap assessments on your behalf, preparedness, define the overlap among the different legislative instruments and give you guidance on how to navigate your way through potential and actual business challenges.

11 There are four series of IEC 62443 standards, aimed at four different Industrial, Automation and Control Systems (IACS) categories: General, Policies & procedures, System and Components. The IEC 62443-4-2 has technical security requirements for IACS components and looks into e.g. identification and authentication aspects, user control and resource availability.
12 CEN and CENELEC's Joint Technical Committee 13 (CEN-CLC/JTC 13) (Work Programme): 'Cybersecurity and Data Protection' will continue the development of harmonized European Standards in support of the Radio Equipment Directive (2014/53/EU), in particular its cybersecurity-related articles 3.3(d), (e) and (f), to become applicable in 2024 *(now postponed to 2025)*. These standards will provide a baseline for cybersecurity for all internet-connected radio equipment. In cooperation with the European Commission, these standards are planned to be cited in the Official Journal of the European Union, thereby guaranteeing manufacturers complying with these standards conformity with the related European legislation.
The anticipated delivery date for the three new CEN/CENELEC standards is now scheduled for 30 June 2024.
13 i.e.: Regulation 2022/30/EU adopted by the EC with a view to enforce the cybersecurity requirements under RED.

PwC contacts

Please contact PwC for more information.
We are more than happy to answer any questions you may have.

Bram van Tiel
Partner Cybersecurity and Privacy,
PwC Netherlands
T: +31 (0)6 22 43 29 62
E: bram.van.tiel@pwc.com

Job van Ommen
Director Cybersecurity and Privacy,
PwC Netherlands
T: +31 (0)6 42 01 78 55
E: job.van.ommen@pwc.com