Cyber Security as a mandatory requirement for radio equipment

The Delegated Regulation (EU) 2022/30 lays down the essential requirements relating to elements of cybersecurity protection according to Art. 3(3) of the RED-Directive 2014/53/EU that must apply from 1 August 2024.

THE CYBER SECURITY REQUIREMENT APPLY TO THE FOLLOWING CATEGORIES OF EQUIPMENT:

- Radio equipment capable of processing personal data or traffic and location data
- Radio equipment designed or intended exclusively for childcare and radio equipment in the scope of toy directive
- Radio equipment that enables the user to transfer monetary values
- Radio equipment designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung from any of the following:
  - i. any part of the human body, including the head, neck, trunk, arms, hands, legs and feet;
  - ii. any clothing, including headwear, handwear and footwear, which is worn by human beings.
- Internet-connected radio equipment (different from the above described specific products)

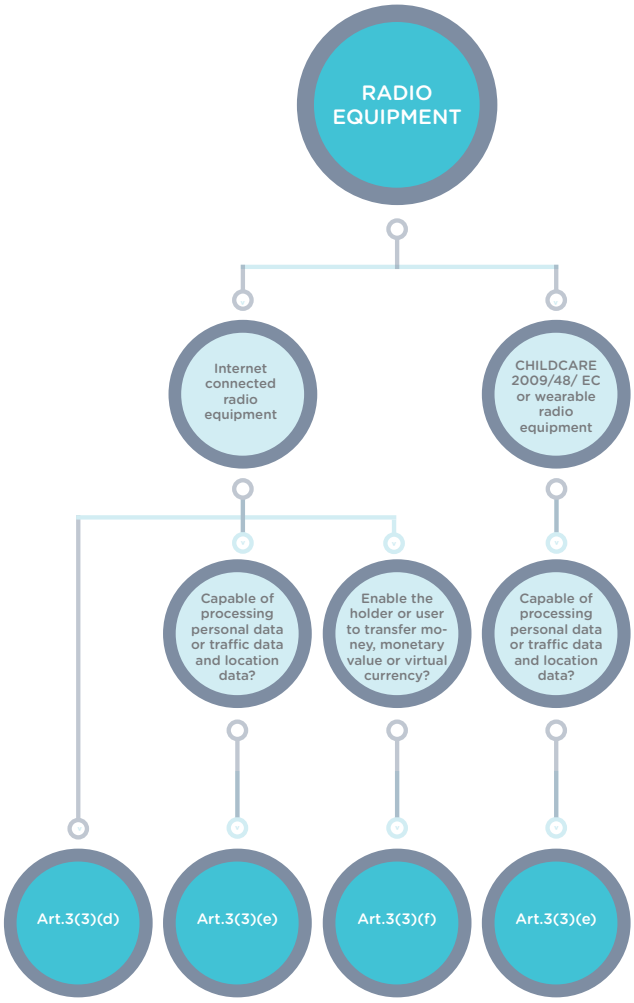
From 1 August 2024 on, all affected devices must comply with both the four classical essential requirements of RED Art. 3.1, Art. 3.2 and those of the relevant subparts of Art. 3(3). The latter are defined as:

(d) No harm to the network or its functioning nor misuse network resources

(e) Protection of personal data and privacy of the user

(f) Protection from fraud

Which of the essential requirements d, e and f apply to a specific device is demonstrated in the following flowchart.



CTC advanced GmbH

Untertuerkheimer Straße 6–10 | 66117 Saarbruecken | Germany | T +49 681 598-0 | F +49 681 598-9075 | mail@ctcadvanced.com | www.ctcadvanced.com

CYBER SECURITY STANDARDIZATION

The draft standardization request foresees three HENs (Harmonized European Norm), one for any of the three new essential requirements to be available 10 months before the date of applicability of the delegated act, so by 1 October 2023. They will include common security requirements addressing a broad range of products and risks. Under favorable conditions, the European Standardization Organizations (ESO) could deliver stable draft versions by the end of 2022. Subsequently manufacturers could use them for conformity assessment in conjunction with a Notified Body involvement. The standardization request specifies technical requirements relevant for each of the three envisaged standards.

Although the detailed structure and content of these standards cannot be proposed by today, the baseline requirements for Cyber Security for Consumer IoT equipment as defined in ETSI's EN 303 645 will serve as key basis for the ESOs work.

EN 303 645 lays down 64 provisions classified into 14 topics:

- **No universal default passwords**
- **Implement a means to manage reports of vulnerabilities**
- **Keep software updated**
- **Securely store sensitive security parameters**
- **Communicate securely**
- **Minimize exposed attack surfaces**
- **Ensure software integrity**
- **Ensure that personal data is secure**
- **Make systems resilient to outages**
- **Examine system telemetry data**
- **Make it easy for users to delete user data**
- **Make installation and maintenance of devices easy**
- **Validate input data**
- **Data protection provisions for consumer IoT**

For some aspects, additional relevant standards will support the process. Following this approach, EN 303 645 can be embedded into a framework taking into account the guidance given in TR 103 621 and the technical recommendation TR 103 701 dealing with the conformance assessment of baseline requirements for Cyber Security. Furthermore, the customer's risk assessment with respect to Cyber Security aspects will also play an important role within the conformity assessment process.

ROUTE TO MARKET

In order to be ready to prepare products in line with the new RED conditions, a pragmatic approach would be helpful, in which the technical requirements listed in the standardization request are transferred to the topics listed before. The result can be a matrix indicating relatively clearly all 64 sub-provisions relevant to the manufacturer's product, albeit with some gaps, of course.

For example, provision 5.1 "No default of password" will be relevant to the requirements set out under Art. 3(3)(d) (e)(f). Provision 5.11 "Make it easy for users to delete user data" however, is not essential for Art. 3(3)(d), but relevant to Art. 3(3)(e) and Art. 3(3)(f). The requirement "Data protection provisions for consumer IoT" cannot be considered as an essential requirement in most cases in the current opinion of the ESOs.

The definition of test cases and assessment for each resulting provision can be derived from the requirements of TS 103 701. In this way, the underlying test methods are clearly described. TR 103 621 provides additional guidance on the implementation of the provisions in EN 303 645 and provides examples illustrating possible solutions.

Finally, it should be emphasized that for conformity assessment all tests free of subjective factors are directly applicable. On the other hand, tests with subjective factors (e.g. tests that consider risks) to be directly applicable under the RED require methodical evaluation by criteria of sufficiency.

We are well prepared to support customers in fulfilling these new requirements. Our specialists are able to respond upon requests and requirements quickly and at any time. They are ready to assist interested parties in preparing their devices to be in line with the upcoming requirements that will be defined in the new standards in the near future.