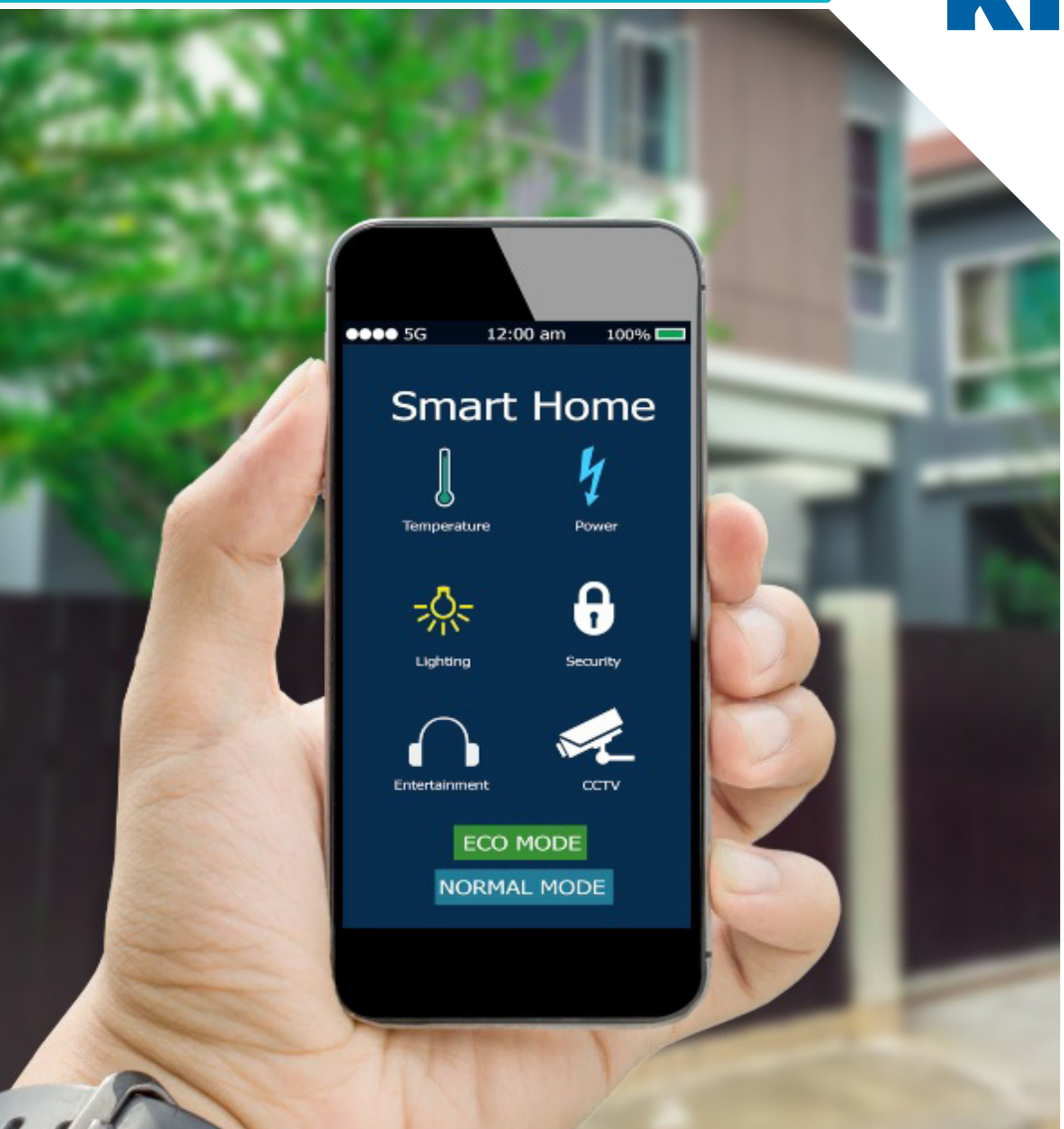
RED Delegated Act on cybersecurity



Kiwa Nederland
Wilmersdorf 50
7327 AC Apeldoorn
The Netherlands

www.kiwa.com

Introduction

On 29th October 2021, EC adopted the RED delegated act activating Article 3.3(d), 3.3(e) and 3.3(f), for both consumer and professional/industrial products (C(2021) 7672 [1]). On 12th of january 2022 this supplement to the RED as been officialy published in the Official Journal.

RED-Directive: 2014/53/EU, Article 3 Essential requirements
Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

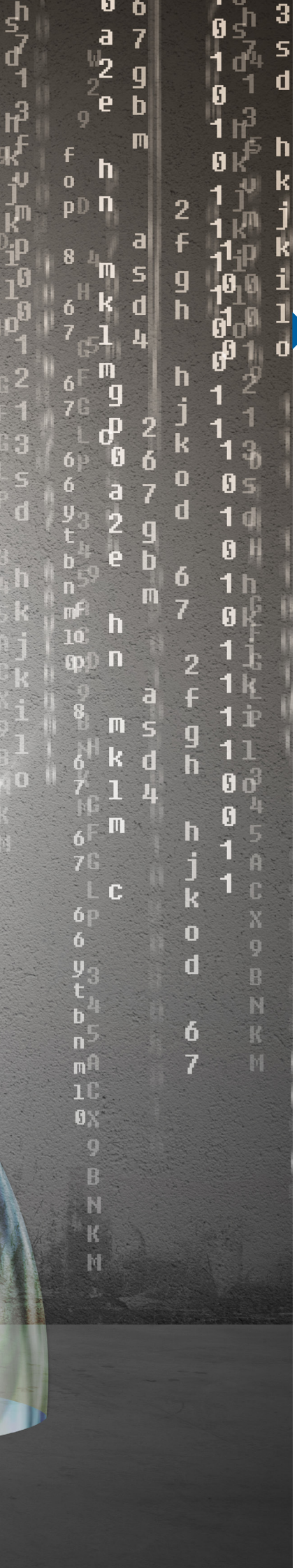
(d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
(f) radio equipment supports certain features ensuring protection from fraud;

By means of this delegated act these 3 subarticles of the RED are now activated and compliance will be mandatory from august 2024.This document is meant to help manufacturers and importers, so they can determine whether it has impact on their organization and if so, determine what there next steps could be.

Additional information:

- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0030&from=EN
- https://ec.europa.eu/growth/news/commission-strengthens-cybersecurity-wireless-devices- and-products-2021-10-29_en including delegated act and related studies)
- https://ec.europa.eu/growth/document/download/492e4668-f9c2-495c-ac11- 4379dd2533d9_en (for delegated act)
- https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_5635 (Q&A)

[1] C_2021_7672_F1_COMMISSION_DELEGATED_REGULATION_EN_V10_P1_1428769



Contents

3. Introduction of subarticles

The Impact of the introduction of article 3.3 depends on which of the subarticles are applicable to your products. In this chapter you are able to find a short discription, an example and a summary of the sub articles in order to define whether this sub article is applicable to your product.

3.1. Introduction of sub article 3.3(d)

3.3(d): radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;

Affects: Radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment').
The device must be capable by itself to communicate over the internet, regardless if it communicates directly or via any other equipment. If the device can make the internet connection by its own, it must fulfil 3.3(d).

For example: If the device communicates to a gateway (gateway makes connection to internet), then the product does not have to comply with 3.3(d). But if connected to a router (the device still makes the connection), than the device must fulfil 3.3(d).

Summary: Affects radio equipment capable of making an internet connection.

3.2. Introduction of sub article 3.3(e)

3.3(e): radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;

Affects: Radio equipment capable of processing (article 4(2)) personal data (article 4(1) of (EU)2016/679 [2]):or traffic data and location data (article 2 (b) (c) of 2002/58/EC [3]):

a. internet-connected radio equipment (other than below)
b. radio equipment designed or intended exclusively for childcare
c. radio equipment covered by Directive 2009/48/EC [4])
d. radio equipment designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung:
    i. any part of the human body, including the head, neck, trunk, arms, hands, legs and feet
    ii. any clothing, including headwear, hand wear and footwear, which is worn by human beings;

Summary: Affects radio equipment where personal data, traffic data and location data is processed.

3.3. Introduction of sub article 3.3(f)

3.3(f): radio equipment supports certain features ensuring protection from fraud;

Affects: Internet-connected radio equipment, if that equipment enables the holder or user to transfer money, monetary value or virtual currency as defined in Article 2, point (d), of Directive (EU) 2019/713. [5]

Summary: affects radio equipment that allows transfer of money or currency.

[2] EU 2016/679: Protection of natural persons with regard to the processing of personal data and on the free movement of such data (repealing 95/46/EC: General Data Protection Regulation)
[3] 2002/58/EC: Processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
[4] 2009/48/EC: Safety of toys
[5] (EU) 2019/713: On combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

4. Impact analysis

According the delegated act C(2021) 7672:

The RED allows the Commission to adopt delegated acts in order to render applicable any of the essential requirements set out in Article 3 (3) of the RED, by specifying each of those requirements that shall concern categories or classes of radio equipment. The three points of the second subparagraph of Article 3 (3) are relevant for this initiative:

- 3(3)(d), to ensure network protection;
- 3(3)(e), to ensure safeguards for the protection of personal data and privacy,
- 3(3)(f), to ensure protection from fraud.

4.1. Analysis 3.3(d)

Manufacturer or importer should do an impact analysis in order to see which (sub) articles are applicable for their product(s). This can be done based on the explanations in chapter 3.

4.2. Analysis 3.3(e)

Manufacturer or importer should do an impact analysis in order to see which (sub) articles are applicable for their product(s). This can be done based on the explanations in chapter 3.

4.3. Analysis 3.3(f)

Manufacturer or importer should do an impact analysis in order to see which (sub) articles are applicable for their product(s). This can be done based on the explanations in chapter 3.

5. Timeline

The COMMISSION'S Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements to which referred to in points (d), (e) and (f) of Article 3(3) of the Directive has been published in the OJEU:

The additional requirements must be met as of 08/01/2024. Untill then manufacturers can make use of a transition period to arrange compliance of their products.

6. What should a manufacturer do? Actions!

Verify if your products are affected by the delegated act and whether the new (sub) article(s) have an impact on your product. If so, please make the necessary preparations and if needed involve your notified body.

In general a manufacturer can show compliance to articles 3.3 d, e & f of the RED by assessing their products according to the IEC 62443-2 or the ETSI EN 303 645 and pass all applicable tests. Kiwa has equipped a state of the art cybersecurity testing laboratory, so that IoT Consumer Electronics as well as industrial IoT components can be tested effectively and efficiently to proof compliance to articles 3.3 d, e and f of the RED.

Products for industrial use:

- IEC 62443-4-2 which specifies the Technical security requirements for IACS (industrial automation and control system) components.

Products for residential use (consumer IoT products):

- ETSI EN 303 645, addressing cybersecurity for the consumer Internet of Things.
  - The ETSI EN 303 645 has a supporting technical standard: the ETSI TS 103 701, Conformance Assessment of Baseline Requirements for consumer IoT.

7. Summary

Objective of the delegated act:
The Commission's initiative aims to achieve the following objectives:

- Make networks more resilient: The equipment will have to incorporate features to avoid their misuse to harm communication networks.
- Improve the protection of personal data and consumers' privacy: The equipment will incorporate features to guarantee the protection of personal data and privacy.
- Reduce the risk of monetary fraud: The equipment will have to include features to minimise the risk of fraud when the equipment is used to make electronic payments.

Applicable to the following products:
In particular, the legislation is applicable to the following equipment:

- Devices capable of communicating via the Internet: Examples of such equipment include electronic devices such as smartphones, tablets, electronic cameras; telecommunication equipment as well as equipment that constitutes the 'internet of things'. Due to insufficient security, such devices present a risk that third parties can improperly access and share personal data, including for fraud purposes, or that such equipment is misused to harm the network.
- Toys and childcare equipment: Toys and baby monitors can be vulnerable to cybersecurity threats that monitor or collect information about children. Therefore, the protection of children's rights constitutes an essential element of this legislation.
- Wearables: Devices like smartwatches and fitness trackers are more and more present in our lives and they collect biometric data.

Why

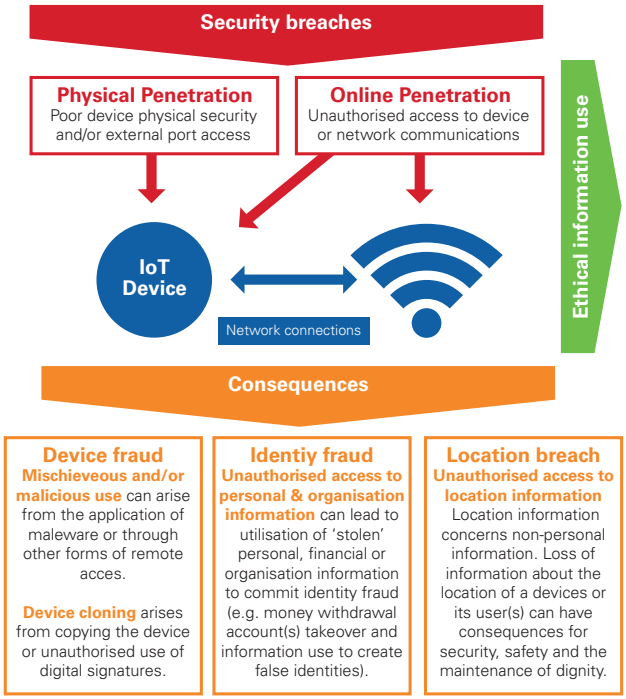


Figure 3.2: Conceptualisation of radio equipment security breaches and consequences

Action to be taken by manufacturers:

Verify if your products are affected by the delegated act and whether the new (sub) article(s) have an impact on your product. If so, please make the necessary preparations and if needed involve your notified body.

For industrial products:

- The IEC 62443-4-2 can be used to fulfill the requirements.

For consumer products:

- The ETSI EN 303 645 can be used to fulfill the requirements.

Mandatory

The COMMISSION'S Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements to which referred to in points (d), (e) and (f) of Article 3(3) of the Directive has been published in the OJEU:

The additional requirements must be met as of 08/01/2024. Untill then manufacturers can make use of a transition period to arrange compliance of their products.

8. Background information for manufacturers:

Overview of topics and provisions discussed in the ETSI EN 303 645.

- Minimise exposed attack surfaces: All devices and services should operate on the 'principle of least privilege;' unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimized to the functionality necessary for the service to operate;
- Make systems resilient to outages: Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, considering the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power;
- Ease of device installation and maintenance: Installation and maintenance IoT devices should employ minimal steps and should follow security best practices on usability. Consumers should also be provided with guidance on how to securely set up their device. No default passwords: Passwords should be unique and not resettable to any universal factory default value;
- Keep software updated: Software components in radio devices should be securely updateable;
- Securely store credentials and security-sensitive data: Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable;
- Communicate securely: Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely;
- Ensure software integrity: Software on devices should be verified using secure boot mechanisms. If an unauthorized change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function;
- Ensure that personal data is protected: Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR) 34. In accordance with GDPR principles, the organizations acting as data controllers must provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes.

Good practice stemming from developing guidelines and Codes of Practice for radio equipment and IoT security would suggest that device manufacturers and IoT service providers should also provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes;

- 33 GDPR requirements will operate when those collecting information become 'controllers of personal data'. This will probably
- arise for most, but not for all ,radio devices.
- Monitor system telemetry data: If telemetry data is collected from devices and services, such as usage and measurement data, it should be monitored for security anomalies;
- Easy personal data deletion: Devices and services should be configured in a way that enables personal data to be easily removed when there is a transfer of ownership, when the consumer wishes to delete the information and/or when the consumer wishes to dispose of a device;
- Validate input data: Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices should be validated. Vulnerability disclosure policy: Companies that provide internet-connected devices and services should provide a public point of contact as part of a vulnerability disclosure policy in order to
- Enable security researchers and others to report issues: This should complement extensive ongoing efforts by the information security community to monitor and document vulnerabilities.

More information

Kiwa is a Notified body for the Radio Equipment directive (RED) and is able to provide assessments and testing according to the IEC 62443 & ETSI EN 303 645. If you have any questions about this document, certification or testing, please contact us via e-mail (cybersecurity.certification@kiwa.com) of phone (+31 (0)88 998 33 70).

Kiwa Nederland
Wilmersdorf 50
7327 AC Apeldoorn
The Netherlands

T. +31 (0)88 998 33 70
E. cybersecurity.certification@kiwa.com
W. www.kiwa.com