RED Delegated Act on cybersecurity

01-11-2022, version 2

Kiwa Nederland
Wilmersdorf 50
7327 AC Apeldoorn
The Netherlands

www.kiwa.com

Introduction

On 29 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 12 January 2022 this supplement to the RED was officially published in the Official Journal of the European Union.

Article 3 of the RED Directive: 2014/53/EU will mandate the following essential requirements regarding cybersecurity

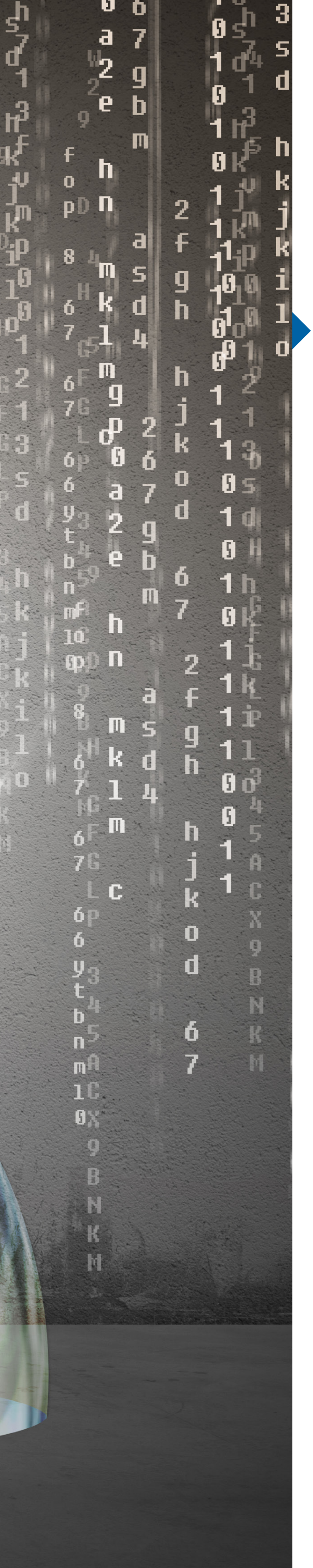
- **(d)** Radio equipment does not harm the network or its functioning nor misuses network resources, thereby causing an unacceptable degradation of service;
- **(e)** Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;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

By means of this Delegated Act these three subarticles of the RED are now activated and compliance will become mandatory from the first of August 2024.This document is meant to support manufacturers and importers to determine the impact on their organization and if so, determine what their 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 the reader is able to find a short description, an example and a summary of the relevant subarticles in order to gather an understanding of what is to come.

3.1. Article 3.3 (d)

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

Impacts: Radio equipment which can communicate over the internet, regardless if it communicates directly or through any other equipment ('internet-connected radio equipment').

The device must be capable by itself to communicate over the internet, either directly or indirectly. If the device can connect to the internet connection on its own, it must fulfill article 3.3 (d).

Example: If the device communicates to a gateway (gateway makes connection to internet), then the product must comply with 3.3 (d). Only if there is no connection to the internet then a device can shun out of compliance to this article.

Summary: Affects radio equipment capable of making an internet connection both directly and indirectly.

3.2. 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.

Impacts: 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]) such as::

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])
    i. Wearables: Devices like smartwatches and fitness trackers are more and more present in our lives and they collect biometric data;

Example: If a product requires personal information of its users to make a user account this article applies. If the personal information is not stored or processed locally on a device, but it is elsewhere (e.g. a remote database) this article also applies.

Summary: Affects radio equipment which processes personal data, traffic data and location data.

3.3. Article 3.3 (f)

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

Impacts: 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]

Example: Products must use sufficient protection features such as encryption, key-exchanges, correct data storage etc.

Summary: The equipment will have to include features to minimise the risk of fraud when the equipment is used to make electronic payments.

Conclusion

Products which will be placed on the European market (e.g. produced or imported from outside of the EU) as of the 1st of August 2024 and meet the capabilities as described in this chapter have to comply with these articles.

[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. How to comply with article 3.3 d) e) & f) of the RED

For compliance to art. 3.3 of the RED, the directive states the following:

'*Where, in assessing the compliance of radio equipment with the essential requirements set out in Article 3(2) and (3), the manufacturer has not applied or has applied only in part harmonised standards the references of which have been published in the Official Journal of the European Union, or where such harmonised standards do not exist, radio equipment shall be submitted with regard to those essential requirements to either of the following procedures: (a) EU-type examination that is followed by the conformity to type based on internal production control set out in Annex III; (b) conformity based on full quality assurance set out in Annex IV.*'

In practice, this means that as long as there is no harmonized standard available, an EU-type examination must be done. This type examination must be performed by a notified body such as Kiwa. The RED defines an EU-type examination as follows:

'*The notified body shall examine the technical documentation and supporting evidence to assess the adequacy of the technical design of the radio equipment. The notified body shall draw up an evaluation report that records the activities undertaken and their outcomes. Where the type meets the requirements of this Directive that apply to the radio equipment concerned, the notified body shall issue an EU-type examination certificate to the manufacturer.*'

In general this means that a notified body performs an assessment when a product fulfills the demands laid down in the RED. As long as there are no harmonized standards, manufacturers must go to a notified body in order to comply with article 3.3 d), e) & f) of the RED.

5. EU Type Examination for article 3.3 d, e and f by Notified Body

The main goal for the type examination is to assess whether the product meets the requirements of articles 3.3 d, e and f. The first step a notified body takes is to examine the product. It is crucial to have a clear understanding of the capabilities and functionalities of the product and its intended use. Based on these three aspects the notified body determines a suitable test plan for checking the compliancy of the product.

Within this phase of determination the notified body draws from available standards which fit the products best and, of course, cover the three sub articles of art. 3.3 of the RED. Several standards can be (partly) combined to create a tailor-made test plan for the conformity assessment of a product.

Once the tests are performed and the product proofs its compliance to all the requirements of the RED art. 3.3, Kiwa issues an RED EU-type examination certificate, mentioning the used standard(s).

E.g.
For consumer IoT equipment a standard which is used often is the ETSI EN 303 645. Though the ETSI EN 303 645 will not be harmonized, the standard entails very useful requirements that can cover all sub articles of art. 3.3 of the RED. Until there is a better standard published this standard is often used.

E.g.
For industrial IoT equipment which is used within industrial automation or control systems a standard which is often used is the IEC/EN 62443-4-2 (the IEC/EN 62443-4-2 also entails compliancy to the IEC/EN 62443-4-1).

6. Development of harmonized standards by the CEN/CENELEC

The European commission has placed a standardization request at the CEN/CENELEC for the development of three new standards, one standard for each sub article (Art.3.3 d), e) & f)). The standards are developed in WG 8 of the JTC 13.

The planned timeline for the development of the new standards is as follows:

- From August 2022 to June 2023: drafting work, HAS consultant assessment, enquiry and comment handling;
- July- September 2023: Formal vote process;
- October 2023: Adoption and publication of the three standards;
- November 2023- July 2024: EC assessment and citation in OJEU;
- 1 August 2024: The DA becomes applicable for all products in scope.

7. Overall generic idea of the requirements as set out for each sub article

Figure 1 depicts the structure put forward by the Delegated Act and the SReq:

- The delegated act (DA) enforces three essential requirements (ER);
- The SReq requests the development and adoption of three new harmonized standards (St.), each of them covering one of the two essential requirements;
- The SReq provides, for each standard to be developed, a series of technical requirements (TR) to be implemented;
- Each standard will then provide, for each technical requirement (TR), detailed product requirements (PR).

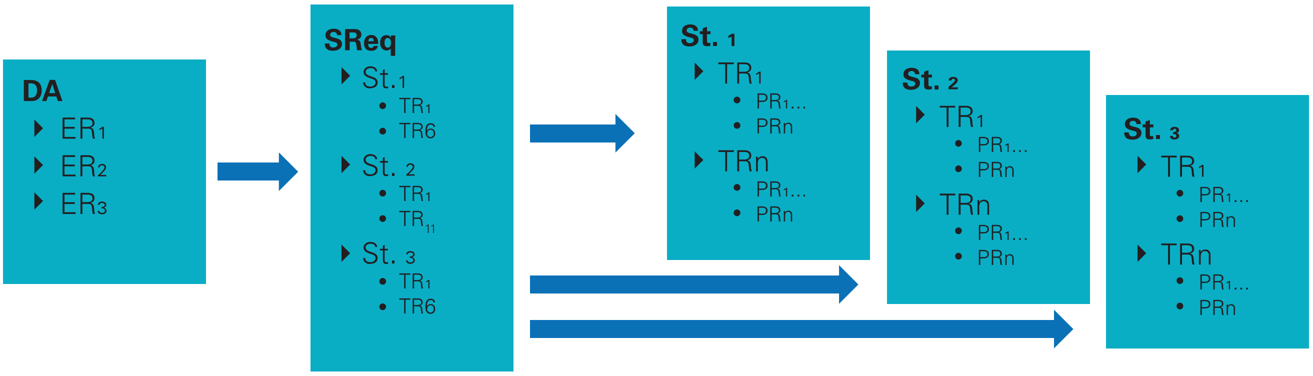


Figure 1. Structure requested by SReq.

The following tables provide an understanding of the aim of each technical requirement (TR) provided in the standardization request. The corresponding product requirements under each technical requirement are still being defined.

However, the partition of the three standards will look like explained below.

Article 3(3)(d) (no harm to network)

Technical requirement	Understanding and considerations
2(1)(a) elements for monitoring and controlling network traffic (including outgoing data)	Prevention of outgoing Denial of Service (DoS) attacks by the equipment itself (after it was corrupted).
2(1)(b) Mitigation of the effects of ongoing DoS attacks	Mitigation of incoming DoS attacks from the internet network (it does not prevent DoS attacks to occur). This requirement does not aim to signal an attack, only to mitigate its impact (e.g. enabling a device to perform its core functions, even when under a DoS attack).
2(1)(c) Authentication and access control mechanisms	Prevention of malware installation (human and machine authentication and assignment of privileges).
2(1)(d) Equipped (risk based) with up-to-date software and hardware without publicly known exploitable vulnerabilities effecting the network	Prevention of malware installation.
2(1)(e) Equipped with automated and secure updating mechanisms for mitigating vulnerabilities potentially harming the network	Installation options for security updates when the equipment is operational.
2(1)(f) Protecting and minimizing exposed attack surfaces	Mitigating effects of successful attacks.

Article 3(3)(e) (protection of privacy)

Technical requirement	Understanding and considerations
2(2)(a) Protecting all kinds of personal digital data against accidental or unauthorized use, loss or unavailability	Self-explanatory
2(2)(c) Equipped with (risk based) up-to-date software and hardware without publicly known exploitable vulnerabilities regarding data protection and privacy	Similar requirement as in 2(1)(d) and (e), but with a different motivation. Here it is about accessing specific personal information, hence different level of risk.
2(2)(d) Equipped with automated and secure mechanisms for updating software or firmware in order to mitigate vulnerabilities that may lead to unauthorized destruction, loss, use or unavailability of personal data.	
2(2)(e) Equipped with functionalities to inform the user of changes that may affect data protection and privacy	Self-explanatory
2(2)(f) Options to log the internal activity that may impact data protection and privacy	This requirement aims to allow for audit trail. This requirement aims to allow the user to keep privacy when reselling, disposing or decommissioning the device. The access levels should fit the authorization level in order to allow such deletion.
2(2)(g) Including functionalities that allow users to easily delete their stored personal data (in order to enable the disposal or replacement of equipment without the risk of exposing personal information)	
2(2)(h) Protecting exposed attack surfaces and minimizing impact of successful attacks	Same requirement as 2(1)(f) above, but different motivation (here it is about accessing specific personal information, hence a different level of risk.

Article 3(3)(f) (fraud protection)

Technical requirement	Understanding and considerations
Where applicable	**Same as above**
2(3)(a) Protection of stored, transmitted or otherwise processed financial or monetary data against accidental or unauthorized access, use, destruction or unavailability	Similar requirement to 2(2)(a) above, but different motivation (here it is about accessing financial or monetary data, hence different level of risk).
2(3)(b) Implementation of appropriate authentication and access control	Same requirement as 2(1)(c) and 2(2)(b) above.
2(3)(c) Equipped with (risk based) up-to-date software and hardware that do not contain publicly known exploitable vulnerabilities regarding financial or monetary data	Similar requirement as in 2(1)(d), (e) and (f) and 2(2)(c), (d), (f) and (h) above with a different motivation (here it is about accessing financial and monetary data, hence different level of risk).
2(3)(d) Equipped with with automated and secure mechanisms for updating software or firmware for mitigating vulnerabilities that may lead to unauthorized storage, access, loss or unavailability of financial or monetary data	
2(3)(e) Options to log the internal activity that may impact financial or monetary data	
2(3)(f) Protection exposed attack surfaces and minimize the impact of successful attacks	

8. Example of roadmap towards art. 3.3 d), e) & f) compliance for manufacturers

1 Determine which products in your product portfolio need to comply with art. 3.3 d) e) & f) of the RED. Use chapter 3 for this analysis.

2 Determine which of your products will still be placed on the European market as from the first of August 2024 (in general, which are produced or imported from outside the EU).

3 Select at least one product within your product portfolio for a pilot and contact a notified body as soon as possible (showing compliance to article 3.3 is a different approach then with the other articles. With the harmonized standards arriving in 2024 at its earliest, it is wise to get acquainted with the procedure, documentation requirements and tests involved for at least one of your products).

4 Perform the assessment together with your notified body and receive your EU-type examination certificate for the product. Use the year 2023 to prepare yourself for the upcoming mandatory requirements.

5 Depending on your situation and the development of the three new standards, determine a test and certification plan for the rest of your product portfolio. Make a (commercial) risk and capability analysis and choose a route to follow. Use the experience you gained during step 4 in this analysis. Consult experts if needed.

6 Complete the route you chose and be compliant before 1 August 2024 for your complete product portfolio.

9. Summary

Compliance to articles 3.3 d, e and f of the RED will become mandatory from the 1st of August 2024. In general terms this means that this will make it mandatory for products entering the EU marketplace to have a baseline of cybersecurity.
For now, there are no harmonized standards available which means the only way to proof compliance to these articles is through a type examination by a Notified Body. Kiwa is already performing assessments for these articles. State of the art standards are utilized to perform type examinations.

However, there are three standards in development by the CEN/ CENELEC which are intended to be harmonized for each of the articles mentioned above.. If these standards are released an harmonized manufacturers can utilize these for self-declaration of compliance in their declaration of conformity (DoC).

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