RED Compliance Association ©

February 2026

Technical Guidance Note (TGN) on the RED compliance requirements for Cyber Security as per Article 3.3(e), processing data and child protection

Title

Contents

1. Introduction

The Radio Equipment Directive 2014/53/EU (RED) applies to radio equipment, as defined in Article 2 of Directive 2014/53/EU.

From 1 August 2025, the cyber security requirements of RED Article 3.3(d), Article 3.3(e), and Article 3.3(f) apply, as detailed in Delegating Act (DA) regulation (EU) 2022/30. The requirements of these Articles apply to any radio equipment in scope of the RED and in scope of those aspects.

Depending on the design and use, a radio equipment may be in scope of any of the following combinations of aspects:

- Article 3.3(d) only
- Article 3.3(e) only
- Article 3.3(d) and Article 3.3(e)
- Article 3.3(d) and Article 3.3(f)
- Article 3.3(d) and Article 3.3(e) and Article 3.3(f)

This Technical Guidance Note (TGN) aims to clarify the requirements of Article 3.3(e), which may include combinations with other Article 3.3 aspects.

2. Scope of TGN

This REDCA TGN has been written for RED Notified Bodies, so that a harmonised approach is used by all RED Notified Bodies when issuing an EU type examination certificate to cover the requirements of RED Article 3.3(e).

This REDCA TGN also provides guidance to manufacturers, installers and test laboratories.

This REDCA TGN deals with the main questions:

- Which radio equipment are in scope of Article 3.3(e)
- Which radio equipment are out of scope of Article 3.3(e)
- Technical Documentation for review by the Notified Body
- Conformity assessment by the Manufacturer and Notified Body
- How to document the information, including the Declaration of Conformity (DoC).

This REDCA TGN deals with radio equipment as per the RED. It is assumed that the manufacturer has already determined that their radio equipment is in scope of the RED, and the remaining question(s) relate specifically to Article 3.3(e).

2.1. Text of RED and Delegating Act regulation (EU) 2022/30

RED, Article 3.3(e):

Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.

Delegated Act regulation 2022/30, Article 1.2:

The essential requirement set out in Article 3(3), point (e), of Directive 2014/53/EU shall apply to any of the following radio equipment, if that radio equipment is capable of processing, within the meaning of Article 4(2) of Regulation (EU) 2016/679, personal data, as defined in Article 4(1) of Regulation (EU) 2016/679, or traffic data, or location data, as defined in Article 2, points (b) and (c) of Directive 2002/58/EC:

(a) Internet connected radio equipment, other than equipment referred to in points (b), (c) or (d)

(b) Radio equipment designed or intended exclusively for childcare

(c) Radio equipment covered by Directive 2009/48/EC

(d) 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, legs, and feet

ii. Any clothing, including headwear, hand wear and footwear, which is worn by human beings

For the purpose of this TGN, all the text in this section, from the RED and the Delegated Act, will be collectively referred to as “Article 3.3(e)”.

3. Definitions

The following definitions apply for the purpose of this REDCA TGN:

3.1. Cyber Security

For the purpose of this TGN, Cyber Security is a generic term used to describe the requirements of RED Article 3.3(d), and/or Article 3.3(e), and/or Article 3.3(f). It is not intended to imply the level of security or resilience associated with the radio equipment.

3.2. 'Internet-connected radio equipment'

Radio equipment in scope of the RED that can communicate itself over the internet, whether it communicates directly or via any other equipment.

In the context of the RED cyber security requirements, the Delegated Act defines "internet-connected radio equipment" as radio equipment which can "communicate itself" over the internet. It does not limit it to equipment which has a direct physical or logical connection to the internet.

ADCO RED has published a document to provide guidance on this topic, and the RED Guide also provides some input on the topic. The following link is valid at the time of writing this REDCA TGN. Please contact the REDCA if this link no longer works:
Interpretation of "internet-connected radio equipment" under the Radio Equipment Directive (RED) | Internal Market, Industry, Entrepreneurship and SMEs

3.3. Communicate itself over the Internet

This requirement applies to any radio equipment within scope of the Delegated Act, which has a capability to send, receive, exchange information, data, and/or messages with other people, systems and/or equipment, using the Internet. It applies to equipment which operates with a protocol (open or proprietary) that allows communication over the Internet.

The radio equipment could achieve this communication directly, or via any other equipment.

If the radio equipment has an IP (Internet Protocol) address, that is a good indication that it is connecting to the Internet and therefore capable of communicating with the Internet. Equipment needs an IP address to connect to the Internet.

The Delegated Act regulation and associated test standards do not limit their applicability exclusively to equipment which has its own IP address. The focus of the regulation is on communication. If a radio equipment does not have an IP address but operates an alternative communication protocol necessary to exchange data with the Internet, the radio equipment could be considered communicating with the Internet, which is relevant to some aspects of Article 3.3(e).

Determining if a radio equipment is communicating over the Internet may not be a simple case of looking at the construction of a product (e.g., type of radio technology or type of protocol) and knowing for sure if it could connect to the Internet.
The radio equipment manufacturer must consider the use cases of their product and determine if it is capable of exchanging information with other people or systems via the Internet, or not.

ADCO RED has indicated that they will focus their attention on equipment which can communicate with the Internet, sending or receiving data, regardless of the connection type.

Note that the word “itself” does not appear in all language translations of the RED Delegated Act. However, recital 5 of the RED Delegated Regulation indicates that the word “itself” means that the radio equipment can connect to the Internet on its own when it operates protocols necessary to exchange data with the Internet, either directly or by means of an intermediate equipment.

It is the manufacturer’s responsibility to determine if their radio equipment can communicate any information or data over the Internet.

3.4. Processing

Regulation (EU) 2016/679 is the General Data Protection Regulation (GDPR).

Within that Regulation, the term “processing” refers to any operation or set of operations performed on personal data, whether manually or automated.

This means any action, large or small, that involves personal data, by computers or by humans.

The GDPR provides a non-exhaustive list of examples, including:

- Collection: Gathering personal data.
- Recording: Creating a record of personal data.
- Organization: Structuring personal data in a systematic way.
- Storage: Keeping personal data in a secure place.
- Use: Employing personal data for a specific purpose.
- Alteration: Changing or modifying personal data.
- Consultation: Accessing or reviewing personal data.
- Dissemination: Sharing personal data with others.
- Erasure: Deleting or removing personal data.

It includes even simple actions like storing or deleting data.

3.5. Personal Data

Regulation (EU) 2016/679 is the General Data Protection Regulation (GDPR).

Within that Regulation, the term “Personal Data” refers to any information relating to an identified or identifiable natural person.

An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

If information can be used to pinpoint a specific individual, it is considered personal data. This includes not only direct identifiers like names and identification numbers but also indirect identifiers that, when combined with other information, could lead to identification. For example, an IP address, while not always directly identifying, can be personal data if the controller has the means to identify the individual behind it. The definition also encompasses information that is not necessarily objective.

Opinions, judgments, and assessments about a person can also be personal data if they relate to an identifiable individual.

3.6. Traffic Data

Directive 2002/58/EC is known as the ePrivacy Directive.

Within that Directive, the term “Traffic Data” refers to any data processed for the purpose of conveying a communication on an electronic communications network or for billing purposes.

This includes data related to the routing, duration, time, or volume of a communication, as well as the type of communication, the location of the sender or recipient's terminal equipment, and the network used. It essentially encompasses the data needed to establish, manage, and bill for a communication.

3.7. Location Data

Directive 2002/58/EC is known as the ePrivacy Directive.

Within that Directive, the term “Location Data” refers to any data processed in an electronic communications network indicating the geographic position of a user's terminal equipment.

This refers to data that identifies the geographical position of a user's device, such as latitude, longitude, or the cell tower serving the device. It may also include the direction of movement or the accuracy of the location information. This type of data is often used to provide location-based services.

Note that this requirement is based on the location of the terminal equipment itself, not of the user.

Note that terminal equipment is used to describe any type of radio equipment and is not restricted to a type of equipment, such as cellular or telephone terminal equipment.

3.8. Childcare

Radio equipment designed or intended exclusively for childcare is a term used to describe radio equipment which may be used by adults to care for children, and/or radio equipment used by children as part of their own activities.

Examples include baby monitors, interactive toys, interactive learning devices, and children’s communication devices such as walkie-talkies and remote-controlled toys.

3.9. Directive 2009/48/EC

Directive 2009/48/EC is the European Union's Toy Safety Directive.

It sets out the essential safety requirements for toys, of health and safety protection for children.

The Directive applies to all toys intended for use by children under 14 years of age. It applies to all toys designed or intended, exclusively or not, for use in play by children under 14 years of age.

3.10. Worn / Wearable

The text of RED Delegated Act regulation 2022/30, Article 1.2 is clear on the conditions associated with this requirement. In this TGN, we use the term “wearable” to refer to those radio equipment described in Delegated Act regulation 2022/30, Article 1.2, and section 2.1 of this TGN, which may be used on the user’s body or clothing.

It may be that body-worn is the only reasonable use of the product, such as earphones or smart glasses. It may be that body-worn is one of the possible uses, such as sports cameras, battery operated satellite navigation, etc.

Clothing can include accessories such as safety helmets and lanyards.

4. Equipment in Scope of Article 3.3(e) – Informative

This section provides informative guidance to the manufacturer and their Notified Body, to help the manufacturer decide if their device is in scope of Article 3.3(e), or not.

For further details and guidance, the RED Guide or the ADCO RED guidance document referenced in section 3.2 of this TGN should be consulted.

4.1. In Scope of Article 3.3(e)

Following the definitions in section 3 of this TGN, the radio equipment in scope of Article 3.3(e) of the RED can be summarised as:

- Radio equipment capable of processing personal data, and/or traffic data, and/or location data, which is Internet connected radio equipment.
- Radio equipment capable of processing personal data, or traffic data and location data, which is designed or intended exclusively for childcare.
- Radio equipment capable of processing personal data, and/or traffic data, and/or location data, which is covered by Directive 2009/48/EC (a toy for children under 14 years of age).
- Radio equipment capable of processing personal data, and/or traffic data, and/or location data, which is designed or intended to be worn on any part of the human body and/or any clothing.

4.2. Not in Scope of Article 3.3(e)

Radio equipment which is excluded from the RED, by RED Annex I.

Radio equipment which is not in scope of the Delegated Act regulation 2022/30, such as medical equipment in scope of Regulation (EU) 2017/745 and/or Regulation (EU) 2017/746, are not in scope of RED Article 3.3(d), Article 3.3(e), or Article 3.3(f).

Radio equipment which is not in the full scope of the Delegated Act regulation 2022/30, such as type approved vehicles, and their systems and components in scope of Regulation (EU) 2019/2144 and Regulation (EU) 2018/1139 or Directive (EU) 2019/520, are not in scope of RED Article 3.3(e) or Article 3.3(f).

Radio equipment which does not meet any of the definitions listed in section 4.1 of this TGN.

4.3. Additional Details

Note that it is not essential for radio equipment to be Internet connected, to be in scope of Article 3.3(e) of the RED. For example, a radio enabled device used by children, which processes personal data but is not Internet connected, would be in scope of RED Article 3.3(e).

5. Conformity Assessment – Normative

The manufacturer's risk assessment must examine the scope of Article 3.3(e) and determine whether or not the radio equipment being assessed is in scope.

If the radio equipment is in scope, the manufacturer must organise an assessment to the essential requirements of Article 3.3(e), which may be performed at a test lab, or cyber security service company or consultant, or by the manufacturer themselves.

The most appropriate cyber security standards available for the RED are generic and broad in scope regarding product types. Therefore, the information supplied by the manufacturer to the assessment lab must detail all the information necessary to accurately assess it.

The manufacturer must describe product details, such as how the equipment operates, if it is password protected, how updates and authentications are performed, the type of technology used to connect to the network, and the specific functions that can be controlled remotely, such as whether remote control is enabled via a mobile app or other interfaces, etc.

The manufacturer's risk assessment must document which standard(s) they choose to apply, and which clauses within the standard(s) apply to their specific radio equipment.
If the manufacturer intends to use a test report to represent models or variants in addition to the tested model, they must provide a clear justification to explain the compliance of the non-tested models, based on the differences and similarities of the models and why the test report is representative of the non-tested models.

5.1. Use of Harmonised Standard

It is possible for manufacturers to fully apply a harmonised standard to show compliance with the RED, for Article 3.3(e).

EN 18031-2: 2024 was listed on the RED OJEU in January 2025. There are restrictions associated with the standard on the OJEU, but it is possible for the manufacturer to avoid these restrictions and fully apply the harmonised standard.

The assessment to the harmonised standard will be based on the product descriptions and details provided by the manufacturer, prior to assessment.

Article 3.3(e) may apply to a range of different product types, and the assessment, and technical documentation, must make it very clear which parts of Article 3.3(e) apply to the radio equipment. For example, it may be in scope because it processes data and can communicate over the Internet, or it may be in scope because it processes data and is body worn, etc.

5.2. Use of Non-Harmonised Standard(s)

It is permitted for the manufacturer to choose an alternative assessment route, without applying the harmonised standard. The manufacturer could partially apply the harmonised standard or could choose a completely different assessment approach.

In addition to the radio equipment details, the manufacturer's risk assessment and technical documentation must match their assessment approach to the essential requirements of the RED, by demonstrating compliance with each part of Article 3.3(e), and showing equivalent compliance to the use of EN 18031-2: 2024.

If not fully applying the harmonised standard, the manufacturer should provide a cross-reference or explanation document to demonstrate how their assessment covers all the requirements, such as by mapping their assessment to the clauses in the harmonised standard.

If not fully applying the harmonised standard EN 18031-2: 2024, the manufacturer must obtain a Notified Body EU-TEC before they can complete their DoC and apply the CE mark.

5.3. Notified Body EU-TEC

For a Notified Body to accept the EU-TEC project based on Article 3.3(e), the Notified Body must be listed on the EC's NANDO website for this capability.

It is not mandatory for the manufacturer to use the same Notified Body for all aspects of the RED. The manufacturer could ask a Notified Body to review Article 3.3(e) based on their expertise in this area, even if they have asked a different Notified Body to review the other RED Articles.

The Notified Body may detail on their EU-TEC the duration and validity of the EU-TEC. A Notified Body's EU-TEC will expire if there are any changes to the standards, the regulations, the state of the art, or the product; regardless of whether that text appears on the EU-TEC or not. See REDCA TGN 29 for more details on this topic.
In the case of an EU-TEC covering Article 3.3(e), the EN 18031-2 standard is not expected to change, but if the manufacturer has applied other standards instead, those could change. Apart from changes to the product, the most significant change is expected to be the arrival of the CRA

on 11 December 2027, when the RED Delegated Act regulation (EU) 2022/30 may become repealed or significantly modified.
The exact transition plans and dates between the RED Delegated Act and the CRA are not confirmed at the time of writing this TGN and therefore a fixed expiry date cannot yet be confirmed. Notified Bodies are recommended and encouraged to add a statement to their EU-TEC which says something like this:

This EU-TEC will expire if there are any changes to the product, the assessment standards applied, the state of the art or the regulation. This EU-TEC will expire if the RED Delegated Act regulation (EU) 2022/30 is repealed, replaced or amended by other legislation, such as the Cyber Resilience Act regulation (EU) 2024/2847.

Notified Bodies are asked to follow this guidance in TGN 36 to ensure harmonisation and consistency between Notified Bodies and the EU-TEC they issue.

6. Technical Documentation and User Information – Normative

The radio equipment manufacturer is always required to create their technical documentation for any radio equipment placed on the market in the EU and EEA, in accordance with Article 21 and Annex V of the RED.

The technical documentation shall contain the manufacturer's RED compliance risk assessment.

When applying to a Notified Body for EU-TEC, the full technical documentation must be supplied. Even if the Notified Body is only examining the radio equipment to the cyber security aspects of the RED, they still require the full set of technical documentation.

Notified Bodies are asked to follow this guidance in TGN 36 to ensure harmonisation and consistency between Notified Bodies and the EU-TEC they issue.

6.1. Technical Documentation

As with all Notified Body applications for EU type examination certificate, the full set of technical documentation must be supplied to the Notified Body. The Notified Body is expected to fully understand the construction and operation of the radio equipment and retain the full technical documentation file for at least 10 years. This explains the reason why the technical documentation submitted to the Notified Body must contain all information about the product, not just the information considered relevant to cyber security.

A manufacturer’s technical operation description or datasheet may need to be expanded for the inclusion of cyber security, to include topics such as: How the radio equipment connects and/or communicates over the network, which functions are enabled through network connectivity, what operations of the radio can be monitored or controlled remotely, how remote access to the radio equipment may be implemented, access passwords, secure update mechanisms, etc.

It is likely that the technical documentation file will need to include new types of documents with the inclusion of cyber security, such as the software bill of materials (SBoM).

As with all aspects of the RED, the technical documentation shall cover all parts and operations of the radio equipment, including non-radio functions, pre-approved radio modules, etc.

If the Notified Body is only being asked to assess the cyber security aspects, for example a review of Article 3.3(e) only, it may not be necessary to submit the test reports related to the other aspects (e.g., safety, EMC, radio test reports), unless the Notified Body asks for them.

The Notified Body is permitted to request any information it considers relevant to their review.

6.2. Risk Assessment

In all cases, the manufacturer's risk assessment should include Article 3.1(a), Article 3.1(b) and Article 3.2 of the RED, plus any applicable aspects in Article 3.3, and possibly Article 3.4.

The manufacturer's risk assessment will document whether or not the radio equipment is in scope of any of the Article 3.3 aspects, such as Article 3.3(e).

If the manufacturer determines that the radio equipment is not in scope of Article 3.3(e), their risk assessment will document why the radio equipment is not in scope. For example, it may detail that the device does not process any of the applicable data types. Or, if it does process data, it does not meet any of the other requirements.

If the manufacturer determines that the radio equipment is in scope of Article 3.3(e), their risk assessment will document which of the parts of Article 3.3(e) apply and therefore explain why it is in scope of Article 3.3(e).

6.3. Declaration of Conformity (DoC)

The manufacturer must create and sign their DoC, applicable to each radio unit that enters the market in the EU or EEA.

If the manufacturer has determined that their radio equipment is in scope of Article 3.3(e), they shall document that on their DoC and list the standard(s) they applied to demonstrate compliance.

If the manufacturer has determined that their radio equipment is not in scope of Article 3.3(e), they do not document that on their DoC. The absence of Article 3.3(e) information on the DoC should indicate that the radio equipment is not in scope of that aspect of the RED.

If a Notified Body has been used to issue an EU-TEC, the Notified Body's name, identification number, and the EU-TEC number shall be listed on the manufacturer's DoC.

Some manufacturers have expressed a concern that if the Cyber Security Article 3.3 aspects are not listed on their DoC, it may not be clear to anyone reviewing the DoC if the manufacturer has deemed the radio equipment to be out of scope, or if they have failed to assess their radio equipment by mistake or intention. However, as the manufacturer is expected to determine whether their radio equipment is in scope based on a worst-case assessment of their radio equipment and its intended use, it should be easy for anyone reviewing the DoC to understand and agree if there is no reference to Article 3.3(e).

If the manufacturer continues to be concerned about this topic, we are not aware of any reason why the manufacturer could not add a simple comment to their DoC, like:
“Article 3.3(e) does not apply to this radio equipment” or simply “Not in scope of Article 3.3(e)”.

Disclaimer
This guidance document does not replace the text of the Radio Equipment Directive and is for guidance only. In legal disputes the text of the Directive or its implementation in National legislation takes precedence.

Annex A – Example Questions

A.1. Personal Data of User or Subscriber

Question: Article 3.3(e) applies to processing of personal data, traffic data and location data. Does it only apply to the data of the user or subscriber? Radio equipment used in corporate or retail environments by company employees may process data which may be personal data, traffic data and location data, but the data is not related to the actual user. The system may not know which employee is using the radio equipment and therefore the data is not personalised. Is the radio equipment in scope of Article 3.3(e) in this case?

Answer: The radio equipment could be in scope. For example, the Article 3.3(e) requirements cover the location of radio equipment and not necessarily the location of the radio equipment user. The radio equipment could be tracking location or traffic data for purposes other than a person.

A.2. Password Use for Special Cases

Question: The Harmonised Standards mandate that a password must be unique or defined by the user, to secure access to the radio equipment. For products such as phones or tablets which are specifically designed for use by the elderly, who may struggle with passwords, is it possible to avoid the password requirement for these devices?

Answer: Each product can be assessed on a case-by-case basis and therefore there could be exceptions to this answer. In general, it would not be appropriate to avoid the requirement for the elderly or others who may struggle with passwords, such as the young, disabled or neurodivergent. These groups can be vulnerable to cyber-attacks and crime; therefore, it is especially important that these people have secure radio equipment. The user may be able to choose a password complexity suited to their abilities and the sensitivity of their data.

A.3. Password Removal After Use

Question: Are manufacturers permitted to have a mandatory password for first use, but then explain in the user manual how the user can remove the password requirement? If the user manual and risk assessment explain that the password is used the first time to meet the RED and then removed by the user, is this acceptable?

Answer: Each product can be assessed on a case-by-case basis and therefore they could be exceptions to this answer. In general, for most normal products it would not be appropriate to allow the user to remove the password requirement after first use. The requirement to have a password has been identified as necessary to protect the user, their data, and the network. The EN 18031 standards do include an option for the user to remove the password, but the EU Commission identified that as a non-compliance with the RED and defined it as a restriction when placing the standards on the OJEU. Removal of the password is effectively allowing the user to put the radio equipment into a mode which is identified by the restriction in the RED OJEU, of allowing the user not to use a password, and therefore no longer compliant with the harmonised standard.

In general, allowing a user to set radio equipment into a non-compliant conditions or modes is not acceptable for any aspects of the RED.

A.4. Article 3.3 not on DoC

Question: If a radio equipment DoC only lists Articles 3.1a, 3.1b and 3.2, with no reference to Articles 3.3(d), 3.3(e) or 3.3(f), how will EU and EEA customs and market surveillance know if the radio equipment is out of scope, or if the manufacturer has failed to assess their radio equipment to the Article 3.3 aspects?

Answer: Most likely the EU and EEA customs and market surveillance will need to solve this with their own assessment and understanding, plus some trust of the manufacturer. For most products, it should be obvious if the Article 3.3 aspects apply. Any radio equipment would be assessed to Article 3.3(e) if it could process personal data. Therefore, it would only be other types of radio equipment that do not have Article 3.3(e) referenced on their DoC.

We are not aware of any regulation to prohibit a manufacturer from declaring on their DoC that an aspect of the RED specifically does not apply.

A.5. Installing Other Software

Question: If a radio equipment, such as a laptop, computer, tablet, smartphone, is sold into the EU and EEA, and allows the user to download additional software or applications (apps) into the equipment which may not meet the requirements, such as passwords, updates, parental control, data tracking, payment authentication, etc. How can the radio equipment manufacturer ensure continued compliance for their equipment?

Answer: As per example A.4. above, this is a tricky situation for the RED which we expect to be resolved by the Cyber Resilience Act (CRA). Radio equipment is assessed by the manufacturer in the condition in which it is placed on the market, and therefore before any modifications are made. If the user installs apps or software which creates modes which are not compliant with the RED, that is the risk of the user, and one which will be resolved under the CRA. As with all RED cases, the radio equipment manufacturer should consider the intended use of their radio equipment and may wish to set guidelines for any app or software installable onto their radio equipment, to only allow authorised apps and ensure that their radio equipment remains compliant in its intended use.

A.6. Scope Disagreement

Question: If a radio equipment manufacturer applies to a Notified Body for an EU-TEC and the Notified Body disagrees with the scope, what are the actions for the Notified Body? For example, if the manufacturer applies Article 3.1 and Article 3.2 but states that the radio equipment is not in scope of Article 3.3, but the Notified Body disagrees and thinks the radio equipment is in scope, what should the Notified Body do?

Answer: The responsibility for application of the RED and CE marking the product lies fully with the manufacturer. The manufacturer has the best knowledge and understanding of how their product operates. For example, if the manufacturer is sure that the radio equipment cannot communicate over the Internet, then they know their equipment best, and it is their decision.

The Notified Body's role is to process the application submitted to them (in this example, to Article 3.1 and Article 3.2 only). The Notified Body may choose to offer guidance and advice to the manufacturer but there is no part of the Notified Body's role relating to mandating how the manufacturer applies the RED to their radio equipment.

A.7. Risk Assessment if Out of Scope

Question: If a radio equipment manufacturer decides that the radio equipment is not in scope of any aspect of Article 3.3 cyber security requirements, is it necessary to mention those aspects in their risk assessment? Is the Risk Assessment only intended to cover the aspects the radio equipment is in scope of?

Answer: The manufacturer's risk assessment should be used to determine which aspects and Articles of the RED apply, and which do not. The risk assessment should include all Article 3.3 aspects (a) to (i), and if the radio equipment is found to be in scope or not. The risk assessment should be used to document why the manufacturer came to that decision.

A.8. Full Technical Documentation for NB EU-TEC

Question: If applying for a Notified Body EU-TEC to cover only partial aspects of the RED, is it necessary to supply the whole technical documentation to the Notified Body? For example, if applying for an EU-TEC to only cover Article 3.3 cyber security, is it necessary to supply the schematics, parts lists, internal photographs, and test reports, if the manufacturer considers that these are not related to cyber security?

Answer: It is necessary to supply the full technical documentation to the Notified Body, even if it may not seem relevant to the manufacturer. The schematics, parts lists, internal photos, user manual, are all used to identify the product, and the Notified Body must retain the technical documentation in their records for at least 10 years after issuing their EU-TEC.

It is quite common that the different RED aspects have separate test reports (for example, a safety test report, an EMC test report, a radio test report, etc.). In this case, it may not be necessary to provide the test reports from the aspects not covered by the EU-TEC. (For example, it may not be necessary to provide the safety, EMC and radio test reports when applying for an EU-TEC covering only the Article 3.3 cyber security requirements. All other documentation is necessary.

A.9. Risk Assessment in Case of Restriction of Harmonised Standards

Question: If a radio equipment does not avoid the restrictions in the harmonised standard, how should that be documented in the risk assessment? For example, if a radio equipment does not implement a password mechanism or uses a default password that cannot be changed by the user.

Answer: One of the purposes of the manufacturer's risk assessment is to identify any compliance risks associated with their product and then document how the manufacturer mitigates the risk. For example, they could identify that a device is in scope of Article 3.3(e) and mitigate the risk by complying with EN 18031-2. However, if the radio equipment cannot comply with an essential

aspect of the standard, or one of the restrictions associated with it, the manufacturer has a couple of options:
The most common route is to fix the issue with their product such that it complies with the standard.
If the radio equipment cannot comply with the standard because of some unique feature or operation of their product, then the manufacturer would detail that clearly in their risk assessment. In the example of the password issue, the manufacturer would use the risk assessment to document how the alternative solutions (mitigations) applied by the manufacturer, or based on the use of the product, provide an equivalent level of protection as would be supplied by meeting the standard and therefore meets the essential requirements of RED Article 3.3(e).

A.10. Password Requirement for Devices Without Passwords

Question: Is it mandatory to implement a password protection for all radio equipment? For example, audio earbuds would not have a password.

Answer: The requirement to have a password which is unique or user defined applies only to products which require password protection, as identified in the EN 18031 standards. There will be radio equipment in scope of Article 3.3(e) which have no user interface or user access, and therefore no requirement for a user password.

A.11. Network which is not Internet connected

Question: Could a home hub or private cellular network be in scope of RED Article 3.3(e), for example a group of radio equipment connected together but not able to communicate with the Internet?

Answer: For radio equipment to be in scope of Article 3.3(e), it is not necessary for Internet communication to exist. In the example of a home hub or cellular network, any of the radio equipment making up the system could be in scope of RED Article 3.3(e) if any of them meet the points detailed in section 4.1 of this TGN.

Disclaimer
This guidance document does not replace the text of the Radio Equipment Directive and is for guidance only. In legal disputes the text of the Directive or its implementation in National legislation takes precedence.