

Brussels, 11 December 2020

## Orgalim comments on the upcoming delegated act for internet-connected radio equipment and wearables

### Executive summary

Orgalim, Europe's Technology Industries, welcomes the opportunity provided by the European Commission to give comments and suggestions with regard to the activation of a delegated act pursuant to Article 3.3 of the Radio Equipment Directive (RED) (sub-articles d),e),f).

First and foremost, we wish to stress that Orgalim members are still of the opinion that a horizontal approach to cybersecurity requirements would be more beneficial than delegated acts, as this would holistically address the risks and concerns related to cybersecurity and ensure the necessary level of protection without creating a patchwork of requirements in product specific legislation.

This paper will, however, only focus on the following three aspects which were raised on 17 November at the RED Expert Group (document EG RE (08)04r01), in order to support the Commission in drafting the delegated act, namely:

- The definition of the scope of the delegated act
- The applicable articles
- The implementation period

## 1. Orgalim comments and proposals

### 1.1. Scope

#### 1.1.1. Connected devices

Orgalim regrets that our proposal of 9 October has not been considered by the Commission as an option in document EG RE (08)04r01. We still consider that the delegated act should cover only those devices that could potentially present cybersecurity risks. Such devices are those able to connect to the internet directly by means of their own public IP address, as they are the only ones which can be publicly visible and potentially accessible by other devices connected to the internet. For this reason, Orgalim requests the Commission to reconsider our proposal submitted on 9 October.

Orgalim would still like to comment on the three options provided in document EG RE (08)04r01 for the definition

of 'connected device', should the Commission consider these as the only ones to be looked at as a way forward.

From our perspective, option 1.c) should be the only one considered. However, Orgalim finds it necessary to modify the definition of 'connected device' as follows:

➤ **Orgalim proposal**

- 'connected device': any radio equipment, falling within the scope of Directive 2014/53/EU, that is ~~capable~~ **intended** to
  - ~~be connected, directly or via another equipment, to internet; **OR**~~
  - ~~use any protocol for the communication of networks of information and communication technologies; **OR**~~
  - be connected **via radio to the internet using** ~~other equipment or a network via any internet communication protocol.~~

➤ **Our argument:**

- The proposed definition for 1.a) and 1.b) has been tailored to the essential requirements for Article 3.3 e) and f), but not d). Moreover, the proposal is not proportionate because it covers more products than only those presenting a cybersecurity risk. That is the case for industrial machinery and automation equipment which is installed in a managed network environment and where security is achieved through a defense-in-depth approach. In such an environment industrial firewalls or specialised internet gateways are placed between the machines and the internet, and they play a vital role in the overall security concept. This scenario is very different from a consumer plug-and-play environment.
- The proposed options 1.b) and 1.c) go beyond '**internet**-connected devices' as they do not refer to the 'internet' anymore. Additionally, option b) brings no value at all because for communication between transmitter and receiver there is always a communication protocol required whether there is a connection to the internet or not. Any definition of 'connected device' in the delegated act should keep the connection to the internet as key to define its scope.
- '**Intended**' should be the main criterion for the application of any RED requirement (references: Article 7, Article 10.8, Article 17). The intention of the manufacturer may well be an exclusively local use of the device without any connection to the internet. This DA should not impose restrictions on manufacturers related to the way their products should be used. Additional unnecessary requirements may create barriers to innovation.
- '**Via radio**': the proposed wording for option 1.c) would bring inconsistency to the application of cybersecurity requirements. A representative example would be a washing machine with LAN and RFID capabilities. In this case, the radio interface has nothing to do with the connection to the internet (RFID interface is used for logistics or maintenance and allows no connection to the internet at all). While the product in this example may indeed fall under the RED (i.e. combined equipment), the DA should only cover the potential risks of the radio connection to the internet. Any radio equipment should only be covered by the DA if it does communicate wirelessly with the internet via any internet communication protocol. 'Via radio' or 'wirelessly' are precisely the criteria proposed by the Commission for wearable devices. Consistency and the same criteria should be ensured for all definitions.
- '**Connection to the internet**' should be the key criterion, not connection to 'products' or 'networks'. There might be cases where the use of IP protocols within fully isolated networks does not represent any risk (e.g. highly secure chemical or manufacturing plants where there is no access to the internet/exterior/public). 'Encapsulation' of a network is a legitimate means to secure a network by default.

## 1.2. Applicable articles and essential requirements

### 1.2.1. Article 3.3 d): internet-connected devices

The Essential Requirement of Article 3.3 d) is: "Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service".

The intention is to protect 'networks', but 'network' is not defined in the RED. The scope of the RED is limited to radio communication and determination in order to protect the radio spectrum. For instance, 'network' in Article 3.2 usually refers to radio (communication) networks. Applying Article 3.3 d) to internet-connected devices creates a different understanding of 'network': instead of radio communication, 'network' is enlarged to the 'internet'.

Furthermore, while the RED may provide the means to protect the radio network where the equipment operates and its functioning, or to avoid misuse of network resources (e.g. spectrum), it is questionable whether these requirements bear any relation to cybersecurity at all. The ultimate goal of Article 3.3 d) is to avoid "causing an unacceptable degradation of service", which is related to the radio performance of the radio equipment. The consideration of Article 3.3 d) in this context would be a departure from its original intent.

#### ➤ Our argument against Article 3.3 d)

- The scope of the RED lays out requirements with respect to radio communication and radio determination to ensure efficient use of the radio spectrum and to avoid harmful electromagnetic interference.  
This is supported by several recitals, e.g. Recital (6)<sup>[1]</sup> or (10), as well by the common understanding and implementation of the predecessor directive (R&TTE directive). In terms of the OSI model (as defined in the ITU-T Recommendation X.200) 'radio communication' would refer to the 'physical layer' – in other words the RED aims to lay out requirements for the physical OSI layer. We underline that this fact is also mentioned in the document of Austria ("EG RE (08)06 - AT Contribution Art 3.3def.pdf").
- Even without the term 'network' explicitly defined in the RED itself it is thus clear that 'network' is used to refer to radio (communications) networks such as in Article 3.2 of the RED itself. Consequently, Article 3.3 d) cannot address the 'internet' (a network using TCP/IP) as a 'network'. Applying Article 3.3 d) to internet-connected devices with the objective of cybersecurity (security within the internet) is not within the meaning of the essential requirement to "not harm the network or its functioning nor [not to] misuse network resources".
- Therefore, we strongly suggest deleting Article 3.3 d) from the list of essential requirements of the future delegated act in order to avoid the risk of crossing the boundaries of the RED.

- **Orgalim proposal:** Orgalim argues that it is sufficient to enforce Articles 3.3 e) and f) to cover cybersecurity. This will also reduce the risk of inconsistent and overlapping requirements.

## 1.3. Date of application

We wish to point out that the essential requirements of Article 3.3 are new requirements for radio equipment which need to be considered and implemented in product planning, design and production. This consideration will in most cases only be possible once the necessary and still-to-be-developed harmonised standards are published and cited in the EU Official Journal (OJ). In this context, it is essential to emphasise the fact that the

---

<sup>[1]</sup> (6) Equipment which intentionally emits or receives radio waves for the purpose of radio communication or radiodetermination makes systematic use of radio spectrum. In order to ensure an efficient use of radio spectrum so as to avoid harmful interference, all such equipment should fall within the scope of this Directive

standardisation mapping done by the Commission is a good starting point. However, existing references are far from being ready to cover a still-to-be-developed standardisation request to the ESOs. The recent RED developments in standardization have shown us the enormous risks that tight periods for standard development bring to the EU market. While the notified body route is seen as an option, their availability and expertise in this new field cannot be compared to the situation of standards under Articles 3.1 and 3.2.

Arguing that ETSI EN 303 645 is already published is not sufficient to solve the problem of releasing standards. The ETSI document is limited to consumer IoT devices. Therefore, significant standardisation work is still to be done to also cover industrial and professional products. IEC 62443-4-2 can be used as a basis, but a lot of work has to be done before achieving a harmonised standard that is fit for supporting the delegated act.

### ➤ **Our argument in support of a longer transitional period**

The industry needs a realistic timeframe to provide EU Internal Market players with the possibility to enjoy presumption of conformity against the new requirements contained within this delegated act. We expect the standardisation and listing process to take three years, and manufacturers need another two years to implement the technical requirements defined in the standard.

We would also like to point out the importance of having at least one harmonised standard cited at the moment the delegated act enters into force. It should consider the following elements:

- having a basis for the presumption of conformity at the design stage;
- allowing a self-declaration of conformity (imposing third-party testing and certification for such additional requirements to the RED is not proportionate);
- In the case of a voluntary assessment with a third party, there will be a risk of unequal and disproportionate understanding of the new essential requirements by the notified bodies before harmonised standards come into force.

Moreover, during this period where there is a lack of harmonised standards, the availability of third parties will become a potential bottleneck causing delays. Therefore, it is important to give sufficient time to standardisation committees, and not to shorten the transition period, in order to generate the necessary harmonised standards and ensure that they are referenced in the corresponding schemes.

- **Orgalim proposal:** Orgalim would like to reiterate the proposal of a transition period of five years before the requirements of the delegated act become applicable. We would also like to note that the periods proposed in EG RE (08)04r01 (18-24 months) are far from being realistic. Should the Commission be certain that the standardisation creation process can be concluded swiftly within 12-18 months, then an absolute **minimum transitional period of 36 months** should be considered. However, to anticipate foreseeable additional delays in the standardisation and citation processes, 60 months would be preferable.

Together with the length of the standardisation process, another reason for the need to have a minimum of 36 months is linked to market surveillance. The Market Surveillance Authorities also need technical guidance in order to achieve an even and proportionate market surveillance. Creating new requirements at a time when the Market Surveillance Authorities do not have the appropriate tools for achieving a legally safe market control is not helpful. The new requirements would theoretically be in force, but not actually enforced.

In addition, transition periods for goods and products with a long life (machines / systems / industrial equipment) should be considered. These products are subject to much longer development cycles compared to consumer products. If covered by the delegated act, a much longer transitional period of 60 months is needed.

## 2. CONCLUSION

In summary, Orgalim has put forward the following concrete suggestions:

- Redefining the scope through an amended definition of 'connected devices', putting the emphasis on the 'connection to the internet' as a key criterion to define radio equipment in the scope of this delegated act.
- Considering only Articles 3.3 e) and f) in the delegated act, and not 3.3 d), as the former would sufficiently cover cybersecurity aspects.
- Proposing a transitional period of five years (i.e. five years after publication – estimated in Q3/2026). If it is the case that the Commission is certain that the standardisation process can be completed in maximum of 18 months, an absolute minimum of 36 months for the transition period is required.

Orgalim represents Europe's technology industries, comprised of 770,000 innovative companies spanning the mechanical engineering, electrical engineering, electronics, ICT and metal technology branches. Together they represent the EU's largest manufacturing sector, generating annual turnover of €2,298 billion, manufacturing one-third of all European exports and providing 11.55 million direct jobs. Orgalim is registered under the European Union Transparency Register – ID number: 20210641335-88.

**Orgalim aisbl**  
BluePoint Brussels  
Boulevard A Reyers 80  
B1030 | Brussels | Belgium

+32 2 206 68 83  
secretariat@orgalim.eu  
www.orgalim.eu  
VAT BE 0414 341 438