DIGITALEUROPE

27 AUGUST 2021

Response to draft Delegated Regulation supplementing Directive 2014/53/EU

Introduction

DIGITALEUROPE appreciates the opportunity to provide its feedback to the European Commission's draft Delegated Regulation under Arts 3(3)(d)–(f) of the Radio Equipment Directive (RED).

In the following comments we expand on:

- The scope of application, particularly with respect to the definition of 'wearable device';
- The applicability of Art. 3(3)(d); and
- The necessary period for the delegated act's entry into application.

This response builds on our previous contributions in the context of the Expert Group on Radio Equipment.[1]

[1] See notably our *Response to EG RE (09)05r01*, March 2021.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Scope

Internet-connected devices

We welcome improvements made in the draft, such as the updated definition of 'internet-connected radio equipment.' With this terminology, devices that could potentially present cybersecurity risks are sufficiently covered.

However, the use of 'can' still appears to capture misuse of equipment beyond what the manufacturer can foresee, which goes beyond Art. 17 RED and the intended use described in the instructions available to the end user.

Proposed changes to Art. 1(1)

The essential requirement set out in Article 3(3), point (d), of Directive 2014/53/EU shall apply to any radio equipment that ~~**can**~~ **is intended to** communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment').

Radio equipment designed or intended exclusively for childcare

We welcome the removal of 'child device.' However, the term 'childcare' is equally ambiguous, with the restriction 'exclusively' also open to interpretation.

We urge again that devices that pose most risks are already covered by the categories of 'internet-connected device' and 'wearable device,' and that we see no need to expand the definition for toy devices.

Proposed changes to Art. 1(2)(b)

~~**(b) radio equipment designed or intended exclusively for childcare;**~~

Wearable devices

A wider scope to all radio equipment designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung from any part of the human body or any clothing seems disproportionate to the identified risks.

While the roadmap pointed out that GPS trackers for kids were an issue as data could be intercepted via the internet, the case study was focused on smart watches and activity trackers. Other wearables (e.g. a small music player attached to clothes, digital cameras strapped around the neck) do not constantly process activity data, health status or communication messages.

Therefore, the delegated act text should revert to the narrower and more restrictive definition put forward in EG RE (09)05r01.

Proposed changes to Art. 1(2)(d)

~~**(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, hands, legs and feet;**~~

~~**(ii) any clothing, including headwear, hand wear and footwear, which is worn by human beings;**~~

Applicable RED articles

Art. 3(3)(d)

Cybersecurity is a moving target, with new vulnerabilities discovered every day even after placement on the market. For this reason, post-market obligations for cybersecurity management are not comparable with current practice with respect to other radio requirements, such as output power and EMC disturbance, which are relatively stable and measurable.

This cannot easily be tackled by a delegated act under an existing directive, and more legal guidance is required before activating this article in particular.

In line with the better regulation objectives, the potential activation of Art. 3(3)(d) should be accompanied by its own impact assessment. We would like to underline that the provisions of Art. 3(3)(d) have not been covered explicitly in the impact assessment. Industry feedback, as a consequence, did not provide specific input regarding this very relevant article.

Art. 3(3)(d) is more related to quality of service, as opposed to the requirements under Arts 3(3)(e) and (f), and the impact of its introduction as well as its relationship with the other two articles was not sufficiently assessed.

Applying ‘harming the network’ beyond the domain of radio communication, which is the scope of the RED, is a significant extension of the RED and creates considerable uncertainty as to how conformity of this article may be assessed. We recommend limiting the interpretation of ‘network’ in Art. 3(3)(d) to apply specifically to the radio network.

The combination of the very broad definition of internet-connected devices and the broadly formulated requirements contained in Art. 3(3)(d) leads to an

impossible task of proving that no misuse can occur, both for manufacturers and for the relevant authorities.

As an example, the delegated act would require that laptops must prevent misuse of the network – any sending of malicious or unproductive packets – while the best cybersecurity today cannot achieve this on a general-purpose machine.

Art. 3(3)(d) has been developed with a view to ensuring radio network protection rather than internet cybersecurity. For such requirements, risk mitigation should be considered rather than defining absolute requirements.

DIGITALEUROPE stresses again that, while we support the need for cybersecurity requirements for products, this should not be achieved by an erroneous activation of the RED, in particular Art. 3(3)(d), and should instead be achieved through more appropriate and coherent horizontal legislation under the New Legislative Framework (NLF), which the Commission itself has announced as upcoming.[2]

Proposed change to Art. 1(1)

delete

We recommend conducting a detailed impact assessment on Art. 3(3)(d) first.

We understand that most stakeholders are of a different opinion. Should the Commission opt not to delete this article, we strongly recommend the inclusion of a recital aiming to prevent contradictions once the planned horizontal legislation comes into force:

(20) Preventing ambiguity in legal requirements on cybersecurity is of great importance for the effectiveness of Union legislation. Therefore, once more comprehensive Union harmonised legislation on cybersecurity enters into force (as announced in 'The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final'), conformity with such legislation should be deemed sufficient for meeting the requirements of this Regulation.

Date of applicability

As evidenced by the input documents from the European standardisation organisations (ESOs) ETSI and CEN-CENELEC during the Expert Group meeting of February 2021, the timeframe for adopting harmonised standards is unrealistic:

[2] JOIN(2020) 18 final.

> *ESOs cannot make reasonable preparation work to identify the requested appropriate HENs for RED containing the right set of verifiable requirements within the expected very short time frame (24 months), and for industry to implement the resulting products.*[3]

> *it appears that the suggested of 18-24 months does not appear practical for the ESOs to deliver harmonised standards.*[4]

In addition, the REDCA, the sectoral group of notified bodies under the RED, indicated that it will be difficult to assess an excessive number of products according to the new essential requirements in case no harmonised standards are available on time.

As harmonised standards are a key tool under the NLF to allow manufacturers to place their equipment on the single market, adequate time needs to be given to the ESOs to adopt good-quality standards.

DIGITALEUROPE appreciates that Recital 18 of the draft delegated act mentions that '[e]conomic operators should be provided with a sufficient time to proceed with the necessary adaptations to classes or categories of radio equipment.' The above statements from the key stakeholders indicate that the standardisation process cannot be achieved in 24 months. In addition to the standardisation work, manufacturers need at least 18 months after the relevant harmonised standards are cited in the Official Journal of the European Union (OJEU) to implement the technical requirements defined in the standard.

In a spirit of compromise, DIGITALEUROPE believes that a date for entry into application should be 42 months after entry into force of the delegated act. This timeframe will strike the right balance between manufacturers' obligations and the urgency stemming from the EU's Cybersecurity Strategy.

Should the Commission nevertheless proceed with the 30-month period, we strongly request that the scope of the standardisation request be limited to minimum baseline requirements only, as was also supported by several Member States.[5] This would be needed in order to avoid disruption of the single market at the time the delegated act applies.

Proposed change

[3] EG RE (09)11.

[4] EG RE (09)10.

[5] See EG RE (02)05r1.

It shall apply from … [OP please insert the date = **~~30~~ 42** months after the date of entry into force of this Regulation].

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Zoey Stambolliu

Policy Officer for Digital Infrastructure

zoey.stambolliu@digitaleurope.org / +32 498 88 63 05

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, ESET, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK