DIGITALEUROPE

10 MARCH 2021

Response to EG RE (09)05r01

Introduction

DIGITALEUROPE appreciates the opportunity to provide its comments on the European Commission's discussion points concerning a delegated act under Arts 3(3)(d)–(f) RED.

DIGITALEUROPE supports a delegated act based on Arts 3(3)(e) and (f) subject to a number of improvements.

In the following comments we expand on:

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

This response reiterates, and builds on, our previous response to EG RE (08)04r01.

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

DIGITALEUROPE welcomes the updated definition of an 'internet-connected device' that communicates itself over the internet. With this terminology, devices that could potentially present cybersecurity risks are sufficiently covered. As the delegated act applies only to radio equipment, we recommend adding that the relevant communication is that which occurs via radio waves.

In addition, the meaning of 'capable of' appears to be not in line with Art. 17 RED, which states that Art. 3(3) only applies to the intended use of the radio equipment. The wording 'capable of' appears to capture misuse of equipment, which goes beyond the intended use described in the instructions available to the end user. Broadening the scope to the possible misuse of radio equipment that could generate cybersecurity risks goes beyond what the manufacturer can foresee.

Proposed changes

(1) 'internet-connected device' means any product or component, falling within the scope of Directive 2014/53/EU, which is ~~***capable***~~ ***intended*** itself to communicate ***via radio*** over the internet, regardless if it communicates directly or via any other equipment;

Child devices

The change from 'toy device' to 'child device' will decrease legal certainty. While the previous definition was clearly aligned with the scope of the Toy Safety Directive,[1] the new definition leads to ambiguity as there is no clear definition of 'childcare.' Similarly, the restriction 'exclusively' can be 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 we see no need to expand the definition for toy devices.

Proposed changes

(2) '~~***child***~~ ***toy*** device' means any product or component, falling within the scope of Directive 2014/53/EU, which is:

[1] Directive 2009/48/EC.

~~*(a)* covered by Directive 2009/48/EC*; or*~~
~~*(b) designed or intended, exclusively, for childcare;*~~

Wearable devices

A wider scope to all wearable devices 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, this definition should revert to the narrower and more restrictive definition put forward in EG RE (08)04r01.

Proposed change

(3) 'wearable device' means any wrist or pocket watch falling within the scope of Directive 2014/53/EU~~*, other than connected devices*~~;

Applicable articles

Art. 3(3)(d)

In line with the better regulation objectives, the potential activation of Art. 3(3)(d) needs to be accompanied by its own impact assessment. 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.

In light of this we would like to underline that the provisions of Art. 3(3)(d) have not been covered explicitly in the impact assessment. Industry was as a consequence not sufficiently informed and could not provide input regarding this article.

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

extensive standardisation proposals lead to a nearly 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 do that on a general-purpose machine.

The RED itself is not written with cybersecurity in mind. 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

Art. 3(3)(d): ***delete***

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

Date of applicability

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

> *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

[2] JOIN(2020) 18 final.

[3] EG RE (09)11.

[4] EG RE (09)10.

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 in order 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 27 of the draft delegated act mentions that 'Economic operators should be provided with a sufficient time to proceed with the necessary adaptations to classes or categories of radio equipment.' The above statements of the key stakeholders indicate that the whole 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 (OJ) 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 24-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.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

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

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

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, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, 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, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

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, Syntec Numérique, Tech in France
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