EUROPEAN
COMMISSION

Brussels, 29.10.2021
C(2021) 7672 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 29.10.2021

supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive

(Text with EEA relevance)

{SEC(2021) 382 final} - {SWD(2021) 302 final} - {SWD(2021) 303 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

Large numbers of radio equipment are used on a daily basis, not only by adult consumers or professional users, but also by vulnerable users like children.

On the one hand, the European Parliament and the Council have repeatedly expressed the need to strengthen Cybersecurity in the EU[1], recognising the growing importance of connected radio equipment, including machines, sensors and networks that make up the Internet of Things (IoT) and the related security concerns. The EU framework is comprised of several pieces of legislation[2] that cover aspects linked to cybersecurity or some of its elements. When addressing certain cybersecurity matters, different actors/stakeholders may have specific obligations to contribute ensuring that the entire ecosystem remains secure. For instance, network operators and service providers should ensure that their systems and platforms are secure, manufacturers of equipment should ensure that it is designed taking into account security principles, users should be aware of risks performing certain operations and of the need of performing the necessary updates of the equipment they use, Member States may establish priorities. Cybersecurity of the entire ecosystem is ensured only if all its components are cyber-secure.

On the other hand, in December 2016, the Norwegian Consumer Council had assessed the technical features of selected radio-connected toys[3]. Its findings point to a possible lack in the protection of children's rights to privacy, personal data protection and security. Thanks to integrated speakers, microphones and other sensors, inter-connected toys are by definition "smart" and can for instance interpret speech, which makes them capable of interacting with the child. They may also record not only photos, videos, geolocalisation data, data linked to the play experience, but also heartrate, sleeping habits or other biometrical data. The report also shows that some of these toys can also advertise products when interacting with the child, which may not be in line with the expected transparency of this kind of products. For this reason, its outcome has made the European Consumer Associations[4] call for action.

---

1 Council conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G, https://www.consilium.europa.eu/media/41595/st14517-en19.pdf
Council conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/connected-digital-single-market/file/cyber-security-package
https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/
http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

2 Notably they are: (i) the General Data Protection Regulation (EU) 2016/679 (GDPR), (ii) the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive, ePD), (iii) the Regulation (EU) 2019/881, the "Cybersecurity Act" (CSA), (iv) the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, "non-cash payment Directive", (v) the Directive 2013/40/EU on attacks against information systems (the 'cyberattack directive'), (vi) the Directive (EU) 2016/1148 on security of network and information systems (the NIS Directive) and (vii) the Regulation (EU) 910 (2014) on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation).

3 https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

4 http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

Toys are just a part of a broader sector, which present similar risks. Directive 2009/48/EC sets out safety requirements that toys covered by the scope of that Directive are to meet before they can be marketed in the Union. The requirements set out in that Directive do not, however, include, for example, requirements, which ensure the protection of personal data and privacy or protection from fraud.

Smart appliances, smart cameras and a number of other connected radio equipment like mobile phones, laptops, dongles, alarm systems and home automation systems are also examples of equipment at risk of hacking and of privacy issues when they are connected to the internet. In addition, wearable radio equipment (e.g. rings, wristbands, pocket clips, headsets, fitness trackers, etc.) can monitor and register a number of the user's sensitive data over time (e.g. position, temperature, blood pressure, heart rate) and retransmit them, not only over the internet, but also through insecure short range communication technologies.The Radio Equipment Directive 2014/53/EU[5] (RED) establishes a regulatory framework for placing radio equipment on the Single Market. It concerns mandatory market access conditions of radio equipment. The RED covers electrical and electronic equipment that can use the radio spectrum for communication and/or radio determination purposes. Member States (MS), via their national market surveillance authorities, shall take corrective measures on non-compliant radio equipment.

Article 3 of the RED sets out the essential requirements that radio equipment placed on the Union market shall comply with Article 3(1)(a) sets out essential requirement in relation to health and safety, Article 3(1)(b) sets out essential requirements in relation to electromagnetic compatibility and Article 3(2) sets out essential requirements in relation to the effective and efficient use of radio spectrum. In addition, Article 3(3) provides for additional essential requirements, which apply to those categories or classes of radio equipment specified in related Commission delegated act (s).

The RED empowers the Commission to adopt delegated acts in order to render applicable any of the essential requirements set out in Article 3 (3) of the RED, by specifying each of those requirements that shall concern categories or classes of radio equipment. The three points of the second subparagraph of Article 3 (3) are relevant for this initiative:

- 3(3)(d), to ensure network protection;
- 3(3)(e), to ensure safeguards for the protection of personal data and privacy,
- 3(3)(f), to ensure protection from fraud.

The aim is, however, not to produce additional or overlapping rules to existing legislation but to ensure that the existing principles, where applicable, are translated into specific requirements for manufacturing goods to be placed on the Union market with a certain degree of enforcement or verifiability. It is important to ensure complementarity with the existing EU framework. In this respect, radio equipment, products or components, to which Regulations (EU) 2019/2144[6] and (EU) 2018/1139[7] or Directive (EU) 2019/520[8] apply should not fall

[5] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, *OJ L 153, 22.5.2014, p. 62–106*

[6] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical

within the categories or classes of radio equipment which should comply with the essential requirements set out in Article 3(3), points (e) and (f), of Directive 2014/53/EU.

As for data protection, Union legislation on personal data and protection of privacy, such as Regulation (EU) 2016/679 of the European Parliament and of the Council[9] and Directive 2002/58/EC of the European Parliament and of the Council[10], regulates the processing of personal data and protection of privacy but does not regulate the placing on the Union market of radio equipment.

The key objective of this initiative is to contribute to strengthen the 'ecosystem of trust' which stems from the synergies of all related pieces of EU law concerning protection of networks, privacy and against fraud, which are better detailed in the accompanying Impact Assessment. This initiative should then allow on the EU market only the radio equipment that is sufficiently secure. With the general objectives in mind, the initiative intends to strengthen the respect of certain fundamental rights (e.g. privacy) and to support the policy objectives laid down in other pieces of EU law that do not allow market enforcement. A timely action is also necessary, given the extent of the risks and considering that a prompt applicability has a positive impact on existing EU policy objectives. The possibility to use existing empowerments that have already been granted to the Commission will allow to act, in respect of the existing framework and without the need of a specific additional legislation. In order to address the problems regarding products lacking security features, a specific objective is to provide market surveillance authorities with an enforcement tool allowing them to take corrective action. Another objective is to ensure a single market in the products concerned, unhampered by diverging local or national regulations that increase administrative burdens for smaller companies in particular. A final objective is to establish a level-playing field through clear and proportionate rules that are effectively and uniformly enforced across the EU.

The necessity for Internal Market rules which include safeguards against insecure products and service is highlighted in the Commission and High Representative of the Union for

---

units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

7 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

8 Directive (EU) 2019/520 of the European Parliament and of the Council of 19 March 2019 on the interoperability of electronic road toll systems and facilitating cross-border exchange of information on the failure to pay road fees in the Union, OJ L 91, 29.3.2019, p. 45.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1

10 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

Foreign Affairs and Security Policy Joint Communication of 16 December 2020 on the EU's Cybersecurity Strategy for the Digital Decade[11].

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

The consultation strategy for this initiative has taken into account all the possible related aspects, also in terms of the impacts for the society (e.g. consumers and economic operators), the national Authorities, the common market access conditions and the implementation of, or synergies with, additional pieces of EU legislation. The feedback provided by stakeholders was used in addition to evidence acquired through other research sources (e.g. desk-research).

The relevant stakeholders were: public Authorities in charge of data processing, frauds and/or radio equipment, associations of economic operators, single economic operators, consumer organisations, citizens, academic/research institutions and relevant non-governmental organisations, notified bodies, European standardisation organisations.

The following specific consultation activities have been carried out:

- All interested stakeholders could provide feedback on the inception impact assessment over a four week period[12];
- A 12-week public consultation has been launched on the Commission's Better Regulation Portal[13];
- A targeted consultation addressed specifically Member States, economic operators (associations or individual), consumer organizations, compliance assessment bodies, consumers or other experts.

Stakeholders were also invited to participate in the targeted survey, including those that have taken part in the Radio Equipment Expert Group meeting. Of these, 56 chose to respond by completing the questionnaire. The 56 respondents came from 20 countries, including 14 EU Member States. The largest number of responses (14) came from Belgium, nearly all of which were bodies representing manufacturers or consumers. Germany was the next best represented country with 11 respondents, most of which were manufacturers. Of the non-EU Member States, the USA was best represented with 5 respondents, which included a mix of manufacturers and industry bodies. There was a balance in the size of organisations responding. Large organisations were all manufacturers or national public administrations, except for two compliance assessment bodies and one university. Many of the micro-organisations were industry or consumer associations. The small and medium sized organisations were a mix of all types of organisation.

A total of 42 respondents completed the open public consultation, which consisted of open and closed questions. The profile of respondents' country was as follows:

[11] JOIN/2020/18 final

[12] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Smartwatches-and-connected-toys

[13] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Smartwatches-and-connected-toys/public-consultation

- The 42 respondents came from 14 EU Member States.
- The largest number of responses (8) came from Germany, of which seven were citizens.
- Six were from Belgium, all of which were EU-level representative bodies (five business associations and one consumer association).
- Six were from Spain, of which four were public authorities and two were companies.
- None of the respondents were located outside the EU.

The profile of the types of respondent was as follows:

- Of the 42 respondents, slightly more than half (22) were citizens.
- Citizens came from 10 EU Member States.
- Of the six public authorities, four were from Spain and one each from Estonia and Ireland.
- Of the seven business associations, five were EU-level bodies based in Belgium.
- The six businesses came from five different countries. Three were micro, two small and one large.
- The one consumer organisation was an EU-level body based in Belgium.

Consultation of the Expert Group on Radio Equipment (E03587) has occurred on preliminary documents addressing key points of the delegated act (scope, applicable Articles, exceptions, date of applicability) on 18th September 2020 and on 17th November 2020. The same Group was consulted in on the draft act on 24th February 2021. The Expert Group on Radio Equipment is participated by Authorities of EU Member States and associated Countries, Consumer Associations, Associations of Economic Operators dealing with the RED, European Standardisation Organisations. Received comments are publicly available in CIRCABC[14], where also the related discussions are summarised in the minutes of the meetings.

A few policy options were either discarded at an early stage, or during the development of this initiative, for different reasons, as below:

- At an early stage, a potential further considered policy option was the introduction of a horizontal piece of legislation on cybersecurity. Several individual manufacturers and their industry associations proposed it as the best policy option which, in their view, would avoid fragmentation of the results, efficiency and effectiveness. It was however pointed out for example in discussions in the Expert Group on Radio Equipment that realistically, given legislative timeframes which are required for a co-decision procedure, such an option may not be as timely as one or more delegated acts under the RED.
- At the time of publishing the Inception Impact Assessment, the Cybersecurity Act was not yet adopted, hence no options could be based on this piece of legislation. Moreover, the establishment of cybersecurity certification schemes under the act

[14] https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/f6e8f574-6864-4350-94bb-1719fe29a6c0?p=1&n=10&sort=modified_DESC

does not create any legal obligations as regards the placement of products on the market. As such, cybersecurity certification remains a voluntary activity and was addressed under the industrial voluntary approaches in the context of policy options.

Finally, at a later stage, i.e. after the publication of the Inception Impact Assessment, certain MS suggested to adopt Article 3(3)(d) in conjunction with Article 3(3)(e) and 3(3)(f), noting the synergies of the adoption of the three articles together. As the MS and the consumer associations considered the adoption of Article 3(3)(d) a complement to option 4, a stand-alone option for Article 3(3)(d) was therefore not considered.

Moreover, to address cybersecurity risks in all connected products and associated services and throughout their entire lifecycle, in the December 2020 Joint Communication on the "EU's Cybersecurity Strategy for the Digital Decade"[15] the Commission announced that it will consider a comprehensive approach, including possible new horizontal rules to improve the cybersecurity of all connected products and associated services placed on the Internal Market.

3. PUBLIC CONSULTATION OF THE DRAFT ACT

After discussing the draft act with the Expert Group on Radio Equipment, a formal 4-weeks public consultation[16] was launched. The consultation was open to all citizens and stakeholders, with no restrictions.

The final number of contributions received was 26. The profile of respondents' country was as follows:

- The largest number of responses (18) came from Belgium.
- Only one contribution was sent from outside the European Union (Switzerland).
- The rest of responses came from the Netherlands (4), Poland (1), Germany (1) and France (1).

The profile of the types of respondent was as follows:

- The majority of the contributions (17) came from the industry.
- Consumers and non-governmental associations provided 3 responses.
- 4 citizens sent feedback.
- 2 contributions were received from the European Standardisation Organisations.

After assessing these contributions, it has been concluded that it is not necessary to modify the draft Act, for the reasons explained below:

- Some contributions specifically addressed technical measures to mitigate cybersecurity threats. However, this Act does not set out technical measures, but it only establishes essential requirements. The opinions expressed in the contributions received on these technical matters will be taken into consideration when developing the supporting harmonised standards.

[15] JOIN/2020/18 final

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Internet-connected-radio-equipment-and-wearable-radio-equipment_en

- Some stakeholders raised concerns on the alleged duplication of obligations with other pieces of EU legislation. This draft Act regulates the placing on the market of the equipment in scope and the rest of the EU legal framework has not regulated this element. In addition, the Act does not intend to regulate any processes or services nor any post-market issues not covered by the Radio Equipment Directive.
- One industry association indicated that, in their view, the Act creates barriers to SMEs. As indicated in the impact assessment, the forthcoming harmonised standards will provide the technical solutions. SMEs will contribute to develop them.
- A number of comments have been received on the understanding of the categories of equipment for which the essential requirements will be applicable. The definition of "internet-connected device" has been discussed at length in the relevant expert group. Limiting the scope in terms of intended use and not of technical capabilities will imply that several equipment would not be covered by the Act. From the technical point of view, communication over the Internet would be possible and hackers could exploit these vulnerabilities. In addition, the concept of "network" is clear and includes the Internet.
- Some industries associations showed concerns about the principle of technological neutrality, as the wired equipment are not covered by the Act. The impact assessment confirms that the wireless devices present a higher risk in terms of cybersecurity and thus, specific policy measures should be implemented for that radio equipment.
- An industry association pointed out that not all the equipment used by children were covered by the Act. In this respect, the protection of children as regards privacy is ensured through the obligations imposed to manufacturers of internet-connected devices, toys and childcare equipment (the last two ones even if they are not capable to communicate over the Internet). Radio equipment used by children is broadly included in the aforementioned categories.
- Finally, the majority of stakeholders showed concerns on the transitional period, being considered too short or too long. The 30-months transitional period is considered to strike the right balance between the need to urgently improve the level of cybersecurity of the radio equipment on the European market and the need to give reasonable time to manufacturers to adapt their products.

4. LEGAL ELEMENTS OF THE DELEGATED ACT

The objective of this delegated regulation is to render applicable the essential requirements set out in Article 3(3)(d), (e) and (f)[17] of the RED, which address elements of cybersecurity, to those categories of radio equipment that pose cybersecurity risks.

More specifically, it provides that Article 3(3)(d), (e) and (f) of the RED shall apply to internet-connected radio equipment, defined in Article 1, subject to certain exclusions as specified in the delegated act.

In addition, it provides that Article 3 (3)(e) of the RED shall apply to wearable radio equipment, toys which are also radio equipment, and radio equipment for childcare, whether internet-connected or not, subject to certain exclusions as specified in the delegated act.

[17] (d) Protection of the network, (e) protection of the personal data and (f) privacy and protection from fraud.

The delegated regulation is coherent with the principles laid down in different relevant pieces of EU legislation, in particular the EU legislation in the area of cybersecurity.

The date of applicability of the delegated regulation is 30 months from its entry into force and the delegated regulation will therefore not affect radio equipment placed on the Union market before that date of applicability.

The delegated regulation has no implications for the EU budget.

COMMISSION DELEGATED REGULATION (EU) …/...

of 29.10.2021

supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC[1], and in particular Article 3(3), the second subparagraph, in conjunction with Article 3(3), first subparagraph, points (d), (e) and (f), thereof,

Whereas:

(1) Protection of the network or its functioning from harm, protection of personal data and privacy of the user and of the subscriber and protection from fraud are elements that support protection against cybersecurity risks.

(2) As stated in recital 13 of Directive 2014/53/EU, the protection of personal data and privacy of users and of subscribers of radio equipment and the protection from fraud may be enhanced by particular features of radio equipment. According to that recital, radio equipment should therefore in appropriate cases be designed in such a way that it supports those features.

(3) 5G will play a key role in the development of the Union digital economy and society in the years to come and will potentially affect almost every aspect of Union citizens' lives. The document with title 'Cybersecurity of 5G networks EU Toolbox of risk mitigating measures'[2] identifies a possible common set of measures which are able to mitigate the main cybersecurity risks of 5G networks and provides guidance for the selection of measures which should be prioritised in mitigation plans at national and at Union level. In addition to those measures, it is very important to follow a harmonised approach to essential requirements relating to elements of cybersecurity protection applicable to 5G radio equipment when it is placed on the Union market.

(4) The level of security applicable under Union essential requirements set out in Article 3(3)(d), (e) and (f) to ensure network protection, safeguards for the protection of personal data and privacy and protection from fraud shall not undermine the high level of security requested at national level for decentralised smart grids in the field of energy where smart meters subject to those requirements are to be used, and for 5G

[1] OJ L 153, 22.5.2014, p. 62.

[2] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 January 2020. https://ec.europa.eu/digital-singlemarket/en/nis-cooperation-group

network equipment used by providers of public electronic communications networks and publicly available electronic communications services within the meaning of in Directive (EU) 2018/1972.

(5) Numerous concerns have also been expressed in relation to increasing cybersecurity risks as a result of the increased use by professionals and consumers, including children, of radio equipment which: (i) is capable itself to communicate over the internet, regardless if it communicates directly or via any other equipment ('internet-connected radio equipment'), i.e., such internet-connected equipment operates protocols necessary to exchange data with the internet either directly or by means of an intermediate equipment; (ii) can be either a toy with radio function which also falls within the scope of Directive 2009/48/EC of the European Parliament and of the Council[3] or is designed or intended exclusively for childcare, such as child monitors; or (iii) is designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung from any part of the human body (including the head, neck, trunk, arms, hands, legs and feet) or any clothing (including headwear, hand wear and footwear) worn by human beings such as radio equipment in the form of wrist watch, ring, wristband, headset, earphone or glasses ('wearable radio equipment').

(6) In this respect, any radio equipment for childcare, radio equipment covered by Directive 2009/48/EC or wearable radio equipment, which is capable itself to communicate over the internet, regardless if it communicates directly or via any other equipment, should be deemed to be internet-connected radio equipment. Implants, for example, should not be considered as wearable radio equipment as they are not worn on, strapped to, or hung from any part of the human body or any clothing. However, implants should be deemed to be internet-connected radio equipment, if they are capable themselves to communicate over the internet, regardless if they communicate directly or via any other equipment.

(7) Given the concerns raised due to the fact that radio equipment does not ensure protection against elements of cybersecurity risks, it is necessary to render applicable, for radio equipment within certain categories or classes, the essential requirements of Directive 2014/53/EU associated with the protection from harm to the network, protection of personal data and privacy of users and of subscribers and protection from fraud.

(8) Directive 2014/53/EU applies to products that meet the definition of 'radio equipment' in Article 2 of that Directive, subject to specific exclusions specified in Article 1(2) and Article 1(3) of that Directive. Whilst the definition of radio equipment in Article 2 of Directive 2014/53/EU refers to equipment that can communicate with radio waves, no requirements of Directive 2014/53/EU make a distinction between the radio and non-radio functions of the radio equipment and therefore all aspects and parts of the equipment should comply with the essential requirements provided for in this delegated regulation.

(9) As regards harm to the network or its functioning or misuse of network resources, unacceptable degradation of services can be caused by internet-connected radio equipment which do not ensure that networks are not harmed or are not misused. For example, an attacker may maliciously flood the internet network to prevent legitimate network traffic, disrupt the connections between two radio products, thus preventing access to a service, prevent a particular person from accessing a service, disrupt a

[3] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p.1).

service to a specific system or person or disrupt information. The degradation of online services can thus result in malicious cyber-attacks, which will lead to increased costs, inconveniences or risks for operators, service providers or users. Article 3(3), point (d), of Directive 2014/53/EU, which requires that radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service, should therefore apply to internet-connected radio equipment.

(10) Concerns have also been raised as regards the protection of personal data and privacy of the user and of the subscriber of internet-connected radio equipment due to the ability of that radio equipment to record, store and share information, interact with the user, including children, when speakers, microphones and other sensors are integrated in that radio equipment. Those concerns relate, in particular to the ability of that radio equipment to record photos, videos, localisation data, data linked to the play experience as well as heartrate, sleeping habits or other personal data. For instance, advanced settings of the radio equipment can be accessed through a default password if the connection or the data are not encrypted or if a strong authentication mechanism is not in place.

(11) It is thus important that internet-connected radio equipment, which is placed on the Union market, incorporate safeguards to ensure that personal data and privacy are protected when they are capable of processing personal data as defined in Article 4(1) of Regulation (EU) 2016/679[4] or data defined in Article 2, points (b) and (c), of Directive 2002/58/EC[5]. Article 3(3), point (e), of Directive 2014/53/EU should therefore apply to internet-connected radio equipment.

(12) Additionally, as regards the protection of personal data and privacy, radio equipment for childcare, radio equipment covered by Directive 2009/48/EC and wearable radio equipment pose security risks even in the absence of an internet connection. Personal data can be intercepted when that radio equipment emit or receive radio waves and lack safeguards that ensure personal data and privacy protection. The radio equipment for childcare, the radio equipment covered by Directive 2009/48/EC and the wearable radio equipment can monitor and register a number of the user's sensitive (personal) data over time and retransmit them through communication technologies that might be insecure. The radio equipment for childcare, the radio equipment covered by Directive 2009/48/EC and the wearable radio equipment should also ensure protection of personal data and privacy, when they are capable of processing, within the meaning of Article 4(2) of Regulation (EU) 2016/679, of personal data, as defined in Article 4(1) of Regulation (EU) 2016/679, or traffic data and location data, as defined in Article 2, points (b) and (c), of Directive 2002/58/EC. Article 3(3), point (e), of Directive 2014/53/EU should therefore apply to that radio equipment.

(13) As regards fraud, information including personal data can be stolen from internet-connected radio equipment, which do not ensure protection from fraud. Specific kinds

---

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

of frauds concern internet-connected radio equipment when they are used to perform payments over the internet. The costs can be high and do not only concern the person who suffered the fraud, but also society as a whole (for example, the cost of police investigation, the costs of victim services, the costs of trials to establish responsibilities). It is therefore necessary to ensure trustworthy transactions and minimise the risk of incurring financial loss of the users of internet-connected radio equipment executing the payment via that radio equipment and of the recipient of the payment carried out via that radio equipment.

(14) Internet-connected radio equipment placed on the Union market should support features for ensuring protection from fraud when they enable the holder or user to transfer money, monetary value or virtual currency as defined in Article 2, point (d), of Directive (EU) 2019/713 of the European Parliament and of the Council[6]. Article 3(3), point (f), of Directive 2014/53/EU should therefore apply to that radio equipment.

(15) Regulation (EU) 2017/745 of the European Parliament and of the Council[7] lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council[8] lays down rules on in vitro diagnostic medical devices. Both Regulations (EU) 2017/745 and (EU) 2017/746 address certain elements of cybersecurity risks associated with the risks addressed by Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU. Radio equipment to which either of those Regulations apply should therefore not fall within the categories or classes of radio equipment which should comply with the essential requirements set out in Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU.

(16) Regulation (EU) 2019/2144 of the European Parliament and of the Council[9] establishes requirements for the type-approval of vehicles, and of their systems and components. In addition, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council[10] is to establish and maintain a high uniform level of civil aviation safety in the Union. Moreover, Directive (EU) 2019/520 of the

---

6 Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (OJ L 123, 10.5.2019, p. 18).

7 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

8 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

9 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

10 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

European Parliament and of the Council[11] lays down the conditions for the interoperability of electronic road toll systems and for facilitating cross-border exchange of information on the failure to pay road fees in the Union. Regulations (EU) 2019/2144 and (EU) 2018/1139 and Directive (EU) 2019/520 address elements of cybersecurity risks associated with the risks set out in Article 3(3), points (e) and (f), of Directive 2014/53/EU. Radio equipment to which Regulations (EU) 2019/2144 and (EU) 2018/1139 or Directive (EU) 2019/520 apply should therefore not fall within the categories or classes of radio equipment which should comply with the essential requirements set out in Article 3(3), points (e) and (f), of Directive 2014/53/EU.

(17) Article 3 of Directive 2014/53/EU provides for essential requirements with which economic operators shall comply. In order to facilitate conformity assessment with those requirements, it provides for a presumption of conformity for radio equipment that complies with voluntary harmonised standards that are adopted in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council[12] for the purpose of expressing detailed technical specifications of those requirements. The specifications will consider and address the level of risks that correspond to the intended use of each category or class of radio equipment concerned by this Regulation.

(18) Economic operators should be provided with a sufficient time to adapt to the requirements of this Regulation. The application of this Regulation should therefore be deferred. This Regulation is not to prevent economic operators from complying with it from the date of its entry into force.

(19) The Commission has carried out appropriate consultations during the preparatory work of the measures set out in this Regulation and has consulted the Expert Group on Radio Equipment,

HAS ADOPTED THIS REGULATION:

Article 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 communicate itself over the internet, whether it communicates directly or via any other equipment (‘internet-connected radio equipment’).

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 and location data, as defined in Article 2, points (b) and (c), of Directive 2002/58/EC:

(a) internet-connected radio equipment, other than the equipment referred to in points (b), (c) or (d);

[11] Directive (EU) 2019/520 of the European Parliament and of the Council of 19 March 2019 on the interoperability of electronic road toll systems and facilitating cross-border exchange of information on the failure to pay road fees in the Union (OJ L 91, 29.3.2019, p. 45).

[12] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(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, hands, legs and feet;

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

3. The essential requirement set out in Article 3(3), point (f), of Directive 2014/53/EU shall apply to any 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.

Article 2

1. By way of derogation from Article 1, the essential requirements set out in Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU shall not apply to radio equipment to which either of the following Union legislation also applies:

(a) Regulation (EU) 2017/745;

(b) Regulation (EU) 2017/746.

2. By way of derogation from Article 1(2) and Article 1(3), the essential requirements set out in Article 3(3), points (e) and (f), of Directive 2014/53/EU shall not apply to radio equipment to which any of the following Union legislation also applies:

(a) Regulation (EU) 2018/1139;

(b) Regulation (EU) 2019/2144;

(c) Directive (EU) 2019/520.

Article 3

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

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

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 29.10.2021

For the Commission
The President
Ursula VON DER LEYEN