EUROPEAN
COMMISSION

Brussels, 29.10.2021
SWD(2021) 302 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

Commission Delegated Regulation

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

{C(2021) 7672 final} - {SEC(2021) 382 final} - {SWD(2021) 303 final}

Table of contents

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT 3
2. PROBLEM DEFINITION 7
   2.1. What are the problems? 9
   2.2. What are the problem drivers? 17
   2.3. How will the problem evolve? 17
   2.4. Impact of COVID-19 19
3. WHY SHOULD THE EU ACT? 21
   3.1. Legal basis 21
   3.2. Subsidiarity: Necessity of EU action 21
   3.3. Subsidiarity: Added value of EU action 22
4. OBJECTIVES: WHAT IS TO BE ACHIEVED? 22
   4.1. General objectives 22
   4.2. Specific objectives 23
5. WHAT ARE THE AVAILABLE POLICY OPTIONS? 23
   5.1. What is the baseline from which options are assessed? 25
   5.2. Description of the policy options 26
   5.3. Discarded options 28
6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS? 29
   6.1. Policy Option 0 – baseline scenario 31
   6.2. Policy Option 1 – voluntary approach 32
   6.3. Policy Option 2 – Article 3(3)(e), focus on protection of privacy and personal data 32
   6.4. Policy Option 3 – Article 3(3)(f), focus on protection from fraud 35
   6.5. Policy Option 4 – Article 3(3)(e) and 3(3)(f), focus on protection of privacy and against fraud 36
   6.6. Policy Option 5 – Article 3(3)(d), 3(3)(e) and 3(3)(f), focus on privacy and fraud protection and network security 43
7. HOW DO THE OPTIONS COMPARE? 47
8. PREFERRED OPTION 50
   8.1. Preferred policy option: option 5 50
   8.2. REFIT (simplification and improved efficiency) 51
9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED? 52

ANNEX 1: PROCEDURAL INFORMATION 54
1. LEAD DG, DECIDE PLANNING/CWP REFERENCES 54
2. ORGANISATION AND TIMING 54

3. CONSULTATION OF THE RSB 54
4. EVIDENCE, SOURCES AND QUALITY 58
ANNEX 2: STAKEHOLDER CONSULTATION 59
Interviews 60
Targeted consultation 61
Open public consultation 62
ANNEX 3: WHO IS AFFECTED AND HOW? 65
1. PRACTICAL IMPLICATIONS OF THE INITIATIVE 65
2. SUMMARY OF COSTS AND BENEFITS 65
ANNEX 4: ANALYTICAL METHODS 68
ANNEX 5: APPLICABLE DELEGATED ACTS 69
ANNEX 6: COHERENCY MAPPING – RELATED PIECES OF EU LAW 70
ANNEX 7: CASE STUDIES 73

1. 1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

This Impact Assessment concerns an initiative to strengthen the cybersecurity of certain categories of radio equipment. The European Parliament and the Council have repeatedly expressed the need to strengthen Cybersecurity in the EU[1] [2] [3], recognising the growing importance of connected devices, 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 that cover aspects linked to cybersecurity or some of its elements. 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)[4]. 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. Currently, however there are no mandatory requirements ensuring the cyber-security of equipment, placed on the EU market. Indeed, the aforementioned pieces of EU legislation neither set out mandatory obligations for manufacturers of equipment which is placed on the EU market, nor allow for corrective measures in case insecure equipment is found on the market.

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 products and allows Member States (MS) to take corrective measures on non-compliant equipment. The RED covers devices that can use the radio spectrum for communication and/or radio determination purposes. It can apply in parallel to other pieces of EU legislation (e.g. on machinery, toys, drones, etc), which focus on the product safety

---

[1] Council conclusions on cybersecurity capacity and capabilities building in the EU, https://data.consilium.europa.eu/doc/document/ST-7737-2019-INIT/en/pdf

[2] the 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

[3] https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/connected-digital-single-market/file/cyber-security-package

[4] Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *OJ L 257*, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

[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*

aspects. All internet-connected radio equipment, including Internet of Things (IoT) with a radio (wireless) function and wearables (such as smart watches) fall under the Directive's scope. As a typical legislation for market access of goods, the RED applies to both consumer and professional products. Equipment that can communicate exclusively by physical means (e.g. a cable) does not fall into the definitions of the Directive and therefore is excluded from its scope. In the specific case of the IoT, the progressive digitalisation and connection to the internet of goods, directly or indirectly, has created over the past years the IoT, which can be defined as in the Recommendation ITU-T Y.2060[6], section 3.2.2, i.e. a "*global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*". The vast majority of the devices comprising the IoT is radio equipment.

In line with the New Legislative Framework ("NLF"), the Directive is based on Article 114 of the TFEU (the approximation of laws)[7]. Article 3(1) and Article 3(2) of the RED set out the essential requirements that all radio equipment in scope of the Directive shall respect in terms of health and safety, electromagnetic compatibility, efficient use of radio spectrum and avoiding harmful interference. In order to support innovation, the RED, in its Annex I, has a specific exclusion for certain equipment used for research and development, specifically "custom-built evaluation kits destined for professionals to be used solely at research and development facilities for such purposes".

Article 3(3) provides the basis for further delegated regulation governing additional aspects by empowering the Commission to adopt acts specifying which categories or classes of radio equipment are concerned by each of the requirements set out in its points (a) to (i) of that Article. The requirements referred to in points (a) to (i) relate to interoperability, emergency services, software, fraud, accessibility, privacy, personal data and misuse of the network. Annex 5 reports the already applicable delegated acts, which so far have been issued under Article 3(3)(g) only. When adopting delegated acts activating the new essential requirements under Article 3(3), a date of applicability has to be specified. This date of applicability needs to provide sufficient time to the manufacturers to adapt their radio equipment to the new essential requirements and demonstrate compliance. Only radio equipment placed on the market after the date of applicability will be subject to the new essential requirements. Radio equipment placed on the EU market before the date of applicability can still be sold in the EU market and does not need to be recalled or modified, provided that it fulfilled the applicable essential requirements at the moment when it was placed on the market.

The three sub-articles relevant for this impact assessment are the following:

- 3(3)(d), to ensure network protection;
- 3(3)(e), to ensure safeguards for the protection of personal data and privacy,
- 3(3)(f), contributing towards 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 EU market with a certain degree of enforcement or verifiability. It is important to ensure

[6] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

[7] Article 114 of TFEU relates to "measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market".

complementarity with the existing EU framework. As regards to this initiative, consequently, a coherency mapping of the already applicable legislation is reported in Annex 6.

In more detail, Article 3(3)(d) of the RED can complement the framework established by the NIS Directive, ensuring that not only the networks *per se* are secure, but also that the connected radio equipment does not harm them. For example, the security of all networks depends on the ability to identify and authenticate each device that is connected to these networks. Without appropriate identification and authentication (features provided by the devices themselves) networks are at risk. Similarly, Article 3(3)(e) can ensure that manufacturers will take into account the "security by design" aspect of the principle of "data protection by design and by default" in the GDPR[8] and the confidentiality of electronic communications in the ePD in designing the equipment. Likewise, Article 3(3)(f) can ensure that manufacturers take the necessary measures to ensure that devices, when used for non-cash payments, support the objectives in the non-cash payment Directive. In a similar manner, the cyberattack Directive defines illegal cyberactivities and lays down obligations to MS to tackle them. The three Articles of the RED mentioned above may complement this framework by introducing mandatory requirements in the equipment which would make it more difficult to perpetrate such activities by means of radio equipment, hence they can support the policy objectives of that Directive. Finally, the basic security assurance referred to in the voluntary cybersecurity schemes developed under the CSA can be a benchmark for the development of technical specifications/harmonised standards in support of the mandatory requirements for market access set out through the RED delegated act. The adoption of a delegated act under Articles 3(3)(d), 3(3)(e) and 3(3)(f) of the RED would represent an action under already granted empowerments, without the need to draft a new piece of EU legislation, which has to follow the co-decision procedure. In particular, the empowerment in the delegated acts under the RED has already been written by the co-legislators. Under this framework, the Commission can specify certain aspects only (e.g. the class or categories of affected products, the date of applicability) and, at the non-opposition of the co-legislators, the acts enter into force and become applicable after an appropriate transitional period. This would be a much faster process than the establishment of a new framework under a co-decision procedure.

A further piece of EU law that may be related to this initiative is the Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. It currently does not address digital aspects, which are addressed under the NIS. However, this piece of legislation is being revised and complementarity will be ensured in case a future revision requires addressing radio equipment connected to the resilience of critical entities.

A number of regulatory and non-regulatory initiatives, mostly at the national level in Europe, as summarised by the European Network and Information Security Agency (ENISA)[9], are being deployed to address different types of security vulnerabilities also identified in connected products. Those initiatives have been developed also in response to reports[10] highlighting concerns on the lack of baseline requirements to ensure a degree of security in these products. In some cases they may impose national requirements on aspects not

[8] "Security by design" is a part of "data protection by design"; the latter term is wider and also covers organisational aspects of ensuring data protection that go beyond what can be achieved on the device level. See also EDPB Guidelines 04/2019 on Data Protection by Design and by Default on how security by design comes in to play here, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

[9] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

[10] https://www.oecd.org/going-digital/topics/digital-consumers/challenges-to-consumer-policy-in-the-digital-age.pdf

covered by EU harmonisation legislation. At the international level, other examples include the UK and its voluntary code of practice relating to consumer IoT security for manufacturers of IoT devices or California and its legislation to regulate consumer IoT security through Senate Bill 327[11]. The latter introduces security requirements for connected devices. It defines them as any device that connects directly or indirectly to the internet and has an IP or Bluetooth address. The Bill provides that, from 1st January 2020, a manufacturer of a connected device is required to equip the device with a "*reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified*".

One recent and very relevant development in the field was the endorsement of the significance of 5G networks to the European economy by the European Council in December 2019 stressing the need to mitigate security risks linked to 5G[12]. As all 5G terminal equipment is radio equipment, it is necessary to ensure that the request of a paramount security is addressed with the existing legislative tools. This initiative is therefore also a complement, on the equipment side and under NLF, to the EU toolbox on 5G Cybersecurity[13] which sets out a coordinated European approach aiming at mitigating the main cybersecurity risks of 5G networks, through coordinated approaches among Member States. The options examined in this impact assessment are fully complementary to that, focusing on the security of equipment connecting to the network.

A further Council Conclusion of 2nd December 2020[14] acknowledges that regulatory measures on certain radio equipment through delegated acts under the RED are a part of a broader strategy to raise the level of cybersecurity of connected devices at Union level. In fact, strengthening the cybersecurity on products will help the protection of the networks. This initiative aims to ensure that certain protection measures implemented on the networks as a result of the provisions of the NIS Directive are not weakened when radio equipment connects to those networks.

Some of the radio equipment covered by this initiative may also fall in the scope of a possible future initiative on the upload of new software on radio equipment pursuant Articles 3(3)(i) and/or 4 of the RED[15]. This other initiative aims to ensure that the level of protection of privacy and against fraud at the moment of placing radio equipment on the market would be maintained with the upload of new software. It will be therefore a further complementing initiative to ensure that the compliance with the RED is demonstrated not only at the moment of initial placing on the market, but also at each upload of software which can impact the essential requirements. Both these initiatives are to be seen in the broader context of developing a legislative framework for Artificial Intelligence (AI), strengthening the applicability of existing "*European legislation on fundamental rights (e.g. data protection, privacy, non-discrimination), consumer protection, and product safety and liability rules*[16]". The aim is, again, to ensure that products placed on the EU market can support,

---

[11] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
[12] https://www.consilium.europa.eu/media/41595/st14517-en19.pdf
[13] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127
[14] https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf
[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2042-Application-of-Article-3-3-i-and-4-of-Directive-2014-53-EU-relating-to-Reconfigurable-Radio-Systems
[16] White Paper on Artificial Intelligence, 19 February 2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

where applicable, the policy objectives laid down in relevant EU legislation and that MS have enforcing tools to ensure it.

In the specific case of "cybersecurity", although the RED does not mention the word, some of its essential requirements in Article 3(3) concern elements of it, such as the protection of the networks (Article 3(3)(d)), the protection of privacy and personal data (Article 3(3)(e)), the protection against fraud (Article 3(3)(f)) and the obligation that software does not compromise the compliance of the equipment that has been demonstrated at the moment of placing on the market (Article 3(3)(i)). Therefore these initiatives are to be seen also in the general context of increasing the cybersecurity in goods that are placed on the EU market.

Numerous MS and consumer associations flagged the absence of certain security features in equipment which is placed on the market - and the consequent risks - to the EU institutions as well as to the members of Telecommunications Conformity Assessment and Market Surveillance (TCAM) Committee, the TCAM Working Group and the Commission Expert Group on Radio Equipment. More specifically, experts as well as international organizations[17] are concerned about the ways personal information and data are collected and shared and how these data may be used for illicit practices. Some MS have brought to the Commission's attention the increasing risks in the area of cybersecurity linked to the increased use of connected products, stressing that it would be beneficial to apply a minimum level of mandatory security to all radio equipment directly or indirectly connected to the internet[18] [19]. As a matter of fact, MS do not have a legislative tool to recall or to impose corrective measures to the equipment that (i) either harms the networks to which it is connected, (ii) does not processes, transmits or stores personal data appropriately, or (iii) does not processes transmits or stores financial data appropriately.

2. 2. PROBLEM DEFINITION

In this section we explain what the problem is (section 2.1), how it originated (section 2.2) and how it is expected to evolve (section 2.3).

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. In December 2016, the Norwegian Consumer Council had assessed the technical features of selected radio-connected toys[20]. Its findings point to a possible lack in the protection of children's rights to privacy 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. They can also be connected to phones/tablets or directly to the internet. The ability of these products to record, store and share information raises concerns related to their safety, security and privacy.

---

[17] https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826 and specifically https://www.oecd-ilibrary.org/docserver/7c45fa66-en.pdf?expires=1537876141&id=id&accname=guest&checksum=9B6F059A453E382BCD1C3A08A03EFB24

[18] https://www.agentschaptelecom.nl/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur

[19] E.g. TCAM WG (12)08 and TCAM WG (14)07, EG RE (02)05, EG RE (02)08

[20] https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

Through a few simple steps, as shown in the report of the Norwegian Consumer Council, a stranger can take control of the toy without having physical access to it, and eavesdrop on and communicate with the child. He/she might be able to track the child or fake the location of the child. 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[21] call for action.

Toys are just a part of a broader sector, which present similar risks. 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 devices (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 short range communication technologies. In the latter case, certain short range communication technologies have been identified as insecure[22] and, as they are used in wearable devices, personal data can be intercepted even in the absence of an internet connection. Therefore, the products concerned by this initiative are "internet-connected and/or wearable radio equipment", a broad category of *radio equipment*, i.e. electronic or electrical product communicating or detecting through radio waves, as per definition in Article 2 of the RED[23]. In the rest of this Impact Assessment, "internet-connected" radio equipment it is intended to be radio equipment that is capable itself to communicate over the internet, regardless if it communicates directly or "indirectly", i.e. via any other equipment.

This category of radio equipment includes not only a number of "conventional" wireless products, such as mobile phones, laptops, wireless cameras, routers, etc., but also "conventional" goods that recently have been provided with a radio function, such as toys, locks, printers, watches, home appliances, and the radio components which allow the connection, in all market segments (e.g. professional, amateur, consumers, industrial, etc.). "Internet-connected radio equipment" refers to radio equipment connected (directly or via another equipment) to the internet. Certain radio equipment that are not connected to the internet, as for instance stand-alone RFIDs (Radio Frequency IDentification), i.e. tags or proximity sensors, would not follow under this initiative, as they are not internet-connected, nor they transmit/process personal or financial data. However, when a specific equipment contains a RFID and that equipment is internet-connected or can transmit/process personal or financial data, the entire product, including the RFID, will fall in the scope of the initiative.

Whilst there are pieces of EU law regulating the general rules for privacy, against frauds or to protect networks or providing for specific actors (e.g. data controllers or MS) to take appropriate measures – see Annex 6 – stakeholders, and in particular Member States and consumer associations, have stressed the absence of legislative tools which would allow to take corrective measures (e.g. fines or withdrawal) against insecure connected products that are placed on the market. Most of these products are wireless or have a

---

[21] http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

[22] https://usir.salford.ac.uk/id/eprint/57465/2/sensors-20-03625.pdf and https://www.cyber.gov.au/sites/default/files/2020-02/Australian%20Government%20Information%20Security%20Manual%20%28Februrary%202020%29_0.pdf

[23] *electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination.*

wireless capability, hence these products as a whole, fall under the scope of the RED. Also products which can be connected through cables but still have at least one wireless capability fall into the scope of the Directive. As explained in the next subsections, there are three kinds of incidents which could be mitigated through delegated acts under the RED, obliging manufacturers to design the equipment in a more secure manner. These concern: the protection of the privacy and personal data, the protection from frauds and the protection of the networks where the equipment operates.

For all the described incidents, numerous studies and reports (see footnotes 8, 9, 16, 17, 19) show or flag shortcomings in products, e.g. presence of default passwords, lack of encryption, and reduced attention to privacy protection in manufacturing. However, there are no data on the technical features of the equipment causing the incidents, specifically whether they are wireless or wired-only products. On a statistical basis, however, it is likely that most of the incidents occur by means of radio equipment, as more and more products have a wireless functionality. For 2021, it is estimated that there will be every 55 wired-connected devices there will be more than 220 wireless-connected devices[24], i.e. radio equipment will account for at least 80% of the connected equipment. On one hand, consequently, not all incidents can be prevented through acting solely on radio equipment, but on the other hand it is likely that this would improve significantly the current situation.

2.1. 2.1. What are the problems?

2.1.1. 2.1.1. Personal data and privacy

As detailed in Annex 6, the protection of privacy is already regulated by other EU legislation. Minimization of data collection, privacy assessments and ensuring a level of security appropriate to the risk are already legal obligations (e.g. in the GDPR) although there are no tools for enforcing these when placing goods on the market, contrary to what is done regarding (physical) safety aspects. The lack of enforcement possibilities at the product level cannot therefore tackle the absence of basic measures such as data encryption and device authentication which would support the policy goals of other pieces of EU legislation.

Consequences of data and privacy breaches are largely dependent on the type and amount of information but can be severe and can result in:

- Identity fraud: Identity fraud occurs from the unauthorized use of one's identity and/or data associated with an identity for fraudulent purposes. It is a specific case of issues which can stem from poor protection of personal data. Identity fraud vulnerabilities during data transfer can arise from poor design of the equipment and lack of sufficient security safeguards.
- Location breach: Location breaches generally concern unauthorised access to location information. Unwanted notification of the location of a user (via wearable devices and transport equipment) or radio equipment in a particular location (home, second home, workplace) can reveal the presence of a known or unidentified person(s). Unauthorised access to information that could identify the lack of presence in a home or location is also a concern (e.g., this information could be of use to those seeking to commit burglaries). For instance, two-way pull-push communication information from an electricity or water smart meter may reveal the absence of a home owner for a prolonged period

[24] see https://www.statista.com/statistics/802711/world-wired-connected-device/ as opposed to https://www.statista.com/statistics/802706/world-wlan-connected-device/

whilst on holiday and it is therefore essential such information is sufficiently protected.

- Geolocational data breaches: Many devices, such as mobile phones and smart watches, incorporate Global Navigation Satellite System (GNSS) and provide real-time information about the location of the user. This is a growing trend where more and more radio equipment, occasionally worn (e.g. a wristband) has the capability of collect and process a vast number of personal data. When the equipment cannot protect the privacy of the transmitted data, the position of the user can be used to put him/her in danger (e.g. children or users that could be a target, such as military personnel).

In the specific case of privacy, according to the guidelines published by the European Data Protection Board (EDPB) on personal data breach notification under the GDPR[25], personal data breaches typically fall in one of the following categories: (1) **confidentiality breaches**: where there is an unauthorised or accidental disclosure of, or access to, personal data; (2) **availability breaches**: where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and (3) **integrity breaches**: where there is an unauthorised or accidental alteration of personal data. In all these cases, the cause can lie in a lack of features in the equipment. When it concerns data related to children, the risks of any breach is even greater. This concerns not only toys, but also products for childcare.

Although in certain cases breaches depend on vulnerabilities that are not related to radio equipment manufacturing (e.g. insecure services, operators' mishandling of data, etc), there is already applicable EU legislation (e.g. the GDPR), which has provisions for manufacturers but does not foresee conditions for market access. Some diligent manufacturers – and other economic operators in their value chain – have already incurred costs to get their products in line with the requirements. Yet, as noted in several studies[26], at the cheaper end of the market, some producers provide low-quality connected radio equipment that lacks minimum levels of protection. This lack of security does not only impact the citizens using them (e.g. with reduced privacy protection), or operators of networks to which these devices are connected (it being easy to interfere with the intended behaviour of this equipment), but represents also a level-playing field issue, as manufacturers providing higher levels of protection may not have sufficient incentives to continue to do so, which in turn risks a race to the lowest level of protection.

Especially Member States and Consumers' Associations believe the problem has grown much worse in the past five years. Therefore low-quality, non-cyber secure products remain on the European single market. The problem had in their view been exacerbated by the trend towards smart and connected products, which is described in section 2.3.

Finally, as regards the implementation of eIDAS, there is currently no commonly agreed methodology for demonstrating compliance. This impacts negatively on the effectiveness and efficiency of the process to achieve mutual recognition and therefore the availability of trusted and secure eID solutions. These weaknesses particularly affect mobile schemes which benefit from high convenience and user uptake. Globally, an increase in demand for digital identity solutions is expected, with a predicted annual market growth ranging from 13%[27] to 20%[28]. Users' expectations with regard to control of personal identity data[29]

---

[25] Guidance available from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
[26] https://www.agentschaptelecom.nl/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur
27 The Insight Partners. (2020). Europe Identity Verification Market to 2027
28 Flood, G. (2019). Global Digital Identity Market to Hit $15BN By 2024. Think.Digital Partners. https://www.thinkdigitalpartners.com/news/2019/05/28/global-digital-identity-market-to-hit-15bn-by-2024/

and effective technologies for fraud and identity theft prevention will increase[30]. Continued growth in mobile penetration strengthens the demand for convenient and secure mobile-first solutions[31].

2.1.2. 2.1.2. Fraud

Frauds can involve a number of criminal activities which can be also related to stealing personal data. The concept is broad and encompasses a plethora of deceitful and criminal actions[32], which can have significant and long-terms impacts on the person who suffered the theft. The costs can be high and do not only concern the person who suffered the fraud, but also society as a whole (e.g. the cost of police investigation, the costs of victim services, the costs of trials to establish responsibilities, etc).

In many cases, frauds are perpetrated in a way that does not concern radio equipment or depend on vulnerabilities that are not related to radio equipment (e.g. insecure services, operators' mishandling of data, etc). However, in certain cases, specific kinds of frauds do concern it, as radio equipment (e.g. smartphones or smartwatches) are used not only to perform non-cash payments over the internet, but progressively also as non-cash means of payment[33]. For instance, smartphone owners have often financial data stored in a digital wallet in their equipment. In turn, this digital wallet allows to transfer money (e.g. to a retailer or a friend) using a near-field communication (NFC) technology embedded in the smartphone. Consumers are progressively enabling this feature in their radio equipment. In this or similar cases, it is then necessary to ensure that radio equipment contains specific features to support trustworthy transactions and minimise the risk that the user can suffer financial damages when using it.

Digital wallets and specific payments details can be stored in the radio equipment and become accessible if no sufficient protection is provided. A low-risk, high-profit criminal activity, is the "card-not-present (CNP) fraud", which occurs largely online, involving the unauthorised use of credit or debit data (the card number, billing address, security code and expiry date) to purchase products and services in a non-face-to-face setting, such as via e-commerce websites or over the telephone. In the majority of cases, the victims are unaware of the unauthorised use of their cards, which remain in their possession. This type of illegal activity has grown steadily, as compromised card details stolen by means of data breaches, certain attacks and data-stealing malware become more readily available on forums, marketplaces and automated card shops in the deep web.

According to the European Central Bank in 2019[34], "*the total number of non-cash payments in the euro area increased by 7.9% to 90.7 billion in 2018 compared with the previous year. Card payments accounted for*

---

29 Deloitte. (2018). Trends in electronic identification: An overview - value proposition of eIDAS eID. European commission.
https://ec.europa.eu/cefdigital/wiki/download/attachments/78549570/Trends%20report%20on%20electronic%20identification_for%20publication_v.1.1.pdf?version=1&modificationDate=1551198712785&api=v2
30. US $50.9bn are expected to be spent on fraud detection and prevention software between 2017 and 2022.30 According to IBM Security and its '2018 Cost of Data Breach Study', the average total cost of a data breach, the average cost for each lost or stolen record (per capita cost), and the average size of data breaches are on the rise and expected to continue growing.
31 Deloitte. (2018). Trends in electronic identification: An overview - value proposition of eIDAS eID. European Commission.
https://ec.europa.eu/cefdigital/wiki/download/attachments/78549570/Trends%20report%20on%20electronic%20identification_for%20publication_v.1.1.pdf?version=1&modificationDate=1551198712785&api=v2
[32] e.g. getting an illicit refund from an insurance, selling goods which are not owned without a mandate, etc.
[33] E.g. through dedicated technologies (e.g. Near Field Communications)
[34] https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2018~c758d7e773.en.html

46% of the total number of non-cash payments in the euro area, while credit transfers and direct debits accounted each for 23%. […] Around 44 billion transactions were processed by retail payment systems in the euro area with an amount of €34.0 trillion" and its fifth card fraud report[35] notes that the total value of card-not-present fraud is increasing: "*With €1.32 billion in fraud losses in 2016, CNP fraud was not only the largest category of fraud in absolute value but, unlike ATM and POS fraud, it was also the only one to record an increase (of 2.1%) compared with the previous year*" and "*Fraud involving cards issued inside SEPA increased for CNP transactions and decreased across the other transaction channels. In 2016 CNP fraud accounted for 73% of total fraud losses on cards issued inside SEPA, compared with 71% in 2015*".

In 2017, the Impact Assessment accompanying the proposal for a Directive of the European Parliament and the Council on combating fraud and counterfeiting of non-cash means of payments[36] has found that

- *"Average loss per fraudulent card transaction: around EUR 130 (result of dividing the value of card fraud, EUR 1440 million, by the number of card transactions, 11.3 million, in 2013).*
- *The average monthly salary in the EU is around EUR 1500 (EUR 1489 in 2014). Losing around 10% of the monthly salary due to fraud (a conservative estimate since there is only card fraud data available) is a significant amount which becomes much more relevant for the citizens earning below the average EU salary (for example, these fraud losses would have represented more than two thirds of the minimum wage in Bulgaria of EUR 173 in 2014);*
- *The probability of a card transaction being fraudulent was 1 in 5000. This was about 4 times more likely than dying on a road traffic accident in the same year, all vehicles combined, and including pedestrians. The most problematic aspect of non-cash payment fraud is that it represents a threat to security. In addition, it is an obstacle to the digital single market.*

The number of credit transfers within the euro area increased in 2018 by 4.7% to 21.0 billion. The relative importance of transactions initiated electronically continued to increase, with the ratio of transactions initiated electronically to paper based transactions now standing at around eleven to one."

Some payment-related frauds have been estimated by the European Central Bank[37] (ECB) and they amount in 2018 to EUR 1.8 billion for cards issued in the Single Euro Payments Area (SEPA), increasing by 8.7% compared to the latest figures available (2013) (EUR 1.44 billion).

As in the case of privacy, there is already applicable EU legislation, but there are no provisions in the "non-cash payment Directive" that concern that the radio equipment placed on the EU market is built according to specific requirements.

2.1.3. 2.1.3. Network protection

As a major enabler for future digital services, 5G and networks of equipment will play a key role in the development of our digital economy and society in the years to come. At the same time, due to the connectivity of digitally enabled conventional goods, a less centralised architecture, and smart computing power of terminal equipment, networks offer more potential entry points for attackers. Therefore, ensuring

[35] https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html
[36] SWD(2017) 298 final https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2017:0298:FIN:EN:PDF
[37] https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html

the security of the EU's future 5G networks and that terminal equipment can be connected without risks of creating harm is of utmost importance. While operators are largely responsible for the secure rollout of 5G, Member States are responsible for national security. Network security is an issue of strategic importance for the entire EU and therefore manufacturers have to contribute to the success of the deployment and security of 5G and other networks.

A significant risk of network attacks exists such as through the use of BotNets[38] if a large number of connected but unprotected devices are hacked. For instance, attacks can occur when fraudsters spread malware through a piece of code in an ad. When a user clicks on that code, the code takes over the user's device and creates a botnet, a network of computers infected without the users' knowledge. Fraudsters then can use this botnet to send spam emails, transmit viruses and engage in other acts of cybercrime, such as Distributed Denial of Services (DDoS)[39] attacks. This botnet risk perpetrated through ad fraud underlies a central threat of IoT frauds. Many newer IoT devices, typically with a wireless connectivity and hence radio equipment, as for instance connected home appliance, do not even have security systems protecting them from botnet attacks. In the same way, ad fraud offers an ideal pathway to creating a botnet because, in general, security intrusions come from perpetrators trying to hack into a system directly, or from perpetrators using a third-party code to try to get into a system indirectly.

A study from F-Secure[40] reports that IoT threats were rarely encountered before 2014, but *"that changed around the time the source code for Gafgyt – a threat that targeted a variety of IoT devices, including BusyBox devices, closed-circuit television (CCTV) devices and many digital video recorder (DVR) devices – was released".*

The ENISA threat landscape for 5G networks[41] stresses that "*mobile communication systems have been prone to security vulnerabilities from their very inception. […] With a growing demand for IP based communications, the fourth generation (4G) enabled the proliferation of smart devices, multimedia traffic, and new services into the mobile domain. This development led to a more complex and dynamic threat landscape. With the advent of the fifth generation (5G) of mobile networks, security threat vectors will expand, in particular with the exposure of new connected industries (Industry4.0) and critical services (connected vehicles, smart cities etc.). […] The integration with and exposure to the data network, is even more prevalent across the 5G network. The growing concerns over availability and protection of user data and privacy will exacerbate with the security challenges introduced by 5G. Hence, the most critical challenges relate to the resilience of the network and the protection of content and metadata of 5G communications".* As the communication occurs between the 5G network infrastructure and the mobile terminals, all being radio equipment, it is then evident that complementing measures need to ensure that the equipment supports the appropriate protection of the networks, without prejudice to further actions to be taken at the network level.

[38] A situation where software applications on different devices run automated tasks perform malicious operations, e.g. Distributed Denial-of-Service (DDoS) attacks or submission of spam, through the internet

[39] An informatics attack aiming to make a server or network resource unavailable to the users, e.g. targeting it with unnecessary requests until it is overloaded.

[40] https://press.f-secure.com/2019/04/01/iot-threats-same-hacks-new-devices/

[41] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

2.1.4. 2.1.4. Interdependences and impact on costs

In general, due to the equipment being vulnerable, consumers, professionals and industry may suffer costs of data breaches. There is a degree of interdependence between privacy protection, prevention of fraud and network protection. There have been many examples[42] of large numbers of insecure internet-connected and/or wearable radio equipment, such as CCTV monitors and baby monitors, being left password unprotected and these vulnerabilities have been exploited through botnet attacks on networks and on individual websites. Hacking into an individuals' home network via a cheap product involves a data breach, which could then expose personal banking details – fraud may be related to the use of personal data, and hacked equipment can be used to produce harm to networks. The inter-linkage between consumer IoT device-level risks and network risks is therefore important and should not be under-estimated.

Several pieces of research provide estimates for costs of data breaches. For example, in the US, IBM and the Ponemon Institute identified the global average cost of a breach as $3.92 million in their 14th joint annual 2019 Cost of Data Breach study[43], though certain industries can have more costly breaches. The study reports that "*the cost of a data breach has risen 12% over the past 5 years and now costs $3.92 million on average. These rising expenses are representative of the multiyear financial impact of breaches, increased regulation and the complex process of resolving criminal attacks. The financial consequences of a data breach can be particularly acute for small and midsize businesses. In the study, companies with less than 500 employees suffered losses of more than $2.5 million on average – a potentially crippling amount for small businesses, which typically earn $50 million or less in annual revenue.*" Among the high-level findings from the IBM / Ponemon study are that 1) Breaches originating from malicious attacks are the most common, accounting for 51% of all breaches, 2) Smaller companies pay disproportionately larger costs in terms of costs per staff member 3) Encryption has the greatest impact on reducing breach costs. The 2018 and 2019 Cost of Data Breaches studies include two new factors in their analysis that influence data-breach costs: deployment of artificial intelligence (AI) and the extensive use of IoT devices. A key finding was that extensive use of IoT devices by organisations increased the risks. It contains data relating to 500 companies globally, of which 115 from Germany, France, Italy, and "Scandinavia"[44]. The 2020 report[45] "*estimates that the cost of a destructive malware attack to companies can be particularly high, with large multinational companies incurring a cost of $239 million per incident, on average*", i.e. "*over 60 times more than the average cost of a data breach*". As the costs of data breaches are assumed to be lower in Europe (less litigious business culture, other economic factors), the assumption is that a typical data breach might cost €100,000 on average for a firm in Europe. This is only an estimate, as the estimates mentioned in surveys and studies vary widely.

Another report[46] concluded that the cost of data breaches will rise globally from $3 trillion each year to over $5 trillion in 2024. This represents an average annual growth of 11%. According to Juniper, *"This will primarily be driven by increasing fines for data breaches as regulation tightens, as well as a greater proportion of business lost as enterprises become more dependent on the digital realm"*. According to

[42] https://www.agentschaptelecom.nl/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur
[43] IBM Security and Ponemon Institute, 2019 Cost of a Data Breach Study: Global Overview July 2019 https://www.ibm.com/downloads/cas/ZBZLY7KL
[44] Denmark, Sweden, Norway and Finland
[45] https://www.ibm.com/downloads/cas/DEDOLR3W
[46] https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches

another research by Verizon, 58% of data breach victims are small businesses, although large firms face particular challenges, as they have large customer databases.

Organisations in transport, manufacturing and healthcare have reportedly suffered substantial losses due to IoT-related vulnerabilities and data breaches. According to a survey based on responses from 700 enterprises in five countries (China, Germany, Japan, UK and US), the average financial impact as a result of an IoT cyberattack was estimated at more than $330,000[47]. However, estimates as to the costs of IoT attacks and of data breaches vary considerably.

A more conservative estimate, which is also based on data available from EU sources, follows a recent (2019) Eurostat survey[48] which shows that 6% of EU companies appear to be affected by destruction or corruption of data following a security incident. The survey concerned companies with more than 10 employees and not in the financial sector (approximately 1.700.000). Even assuming that the micro enterprises did not suffer any loss due to data breaches, it can be estimated that 100.000 companies suffered data breaches. Taking the above average cost of data breaches (100.000 EUR), the costs for data breaches can be conservatively estimated to at least EUR 10 billion per year. This number is confirmed as a low-bound estimate by looking at the approximately 90.000 breaches – concerning the GDPR only – which were reported in 2019[49].

Even if data breaches do not occur, the costs of DDoS attacks can be high: in 2016 Kaspersky estimated[50] that *"other major DDoS-related costs included PR expenses to restore a company's reputation (9%), upgrading IT infrastructure and software (10%), staff training (10%) and customer compensation (12%). This can bring the average cost of a DDoS attack to about $106,000 for smaller companies and more than $1.6 million for large enterprises."* It also reported that "*DDoS attacks are one of the most expensive cyberthreats for companies. […] There have been incidents where prolonged DDoS attacks have led to the bankruptcy and closure of successful online businesses*". The estimates of 2017[51] showed that "*the financial implications of reacting to a DDoS attack in 2017 is $123K for SMB*[52]*s, compared to $106K in 2016. For enterprises, the cost has soared to more than half a million dollars – from $1.6M in 2016 to $2.3M in 2017, on average*".

CISCO estimates that approximately 10.8 million DDoS attacks will occur globally in 2020[53]. Considering the ratio of the population[54], 600.000 DDoS will likely concern EU companies. Recalling the costs of each DDoS ($123.000 or approximately EUR 110.000), the overall costs in the EU due to DDoS can be estimated to be in the order of EUR 65 billion. 600.000 companies represent approximately 2.4% of all EU companies.

---

[47] Irdeto Global Connected Industries Cybersecurity Survey https://irdeto.com/news/new-2019-global-survey-iot-focused-cyberattacks-are-the-new-normal/.
[48] Community Survey on ICT Usage and e-Commerce in Enterprises, the sample is considered representative (almost 160,000 businesses), see https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisce_ic&lang=en
[49] https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf
[50] https://www.kaspersky.com/about/press-releases/2016_lose-a-fortune-one-ddos-attack-can-cost-a-company-over-1.6m
[51] https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report
[52] small and medium businesses
[53] https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
[54] ratio of the EU27 and global population

The recent Eurostat survey[55] also covers the unavailability of ICT services for companies with more than 10 employees and not in the financial sector following a security incident, which are exemplified as "DDoS, ransomware attacks, hardware or software failure, theft". It shows that 10% of the surveyed EU companies suffered unavailability of ICT services following a security incident, at least once. Considering the differences in scope of the threats between the two sources, the percentage of affected companies in the two sources do not appear to be in contradiction.

Loss of personal or financial data, and suffering disruption of services can impact on the reputation of companies. Reputation can account to 25% of the value of a company[56] and trust plays a significant role in the willingness of users and customers to pay a premium[57]. Costs related to reputational damage could not be estimated, but the interview programme run by the Commission's contractor with manufacturers in the related Impact Assessment Study[58] also found that leading European manufacturers in some product groups for internet-connected and/or wearable radio equipment are investing significant resources in strengthening product security to enhance their brand's reputation, by building security into their value proposition. Whilst a percentage of their investment in improving product security is made for regulatory compliance reasons, the primary reason for focusing on security is to embed it within their marketing. However, not all equipment will have minimum common protections. Consumers associations have been repeatedly invoking[59] the need of baseline mandatory requirements, and some of them may underestimate the importance of network security, as it is not a matter they perceive. In 2019, the European Court of Auditors[60] confirmed that "*Citizens are often vectors for attacks […], since they are likely to be unwittingly exposed to vulnerabilities in cheap and widely distributed devices and software […]*" and "*the exponential growth of the Internet of Things, the cloud, big data and the digitisation of industry is accompanied by a growth in the exposure of vulnerabilities, enabling malicious actors to target ever more victims. The variety of attack types and their growing sophistication make it genuinely difficult to keep pace. Malware (malicious software) is designed to harm devices or networks*". It is consequently paramount to increase the security – and the security of radio equipment, for what it concerns this initiative – as an important component of value, reputation and trust.

Perceived security is an enabler to the digital transformation and non-action can have, consequently, a negative impact. Recent research[61] has investigated consumer trust purchasing behaviours. The result is that consumers are ready to pay, on average, between 30% and 40% more for equipment with demonstrated security features (a label in the study). The Commission contractor's estimate[62] was more conservative and estimated between 10% and 20% would pay extra for more secure products. However, this depends what is taken as the baseline comparator. For example, a consumer might purchase a better quality product with

---

[55] https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisce_ic&lang=en
[56] Deloitte https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-reputation-matters-june-2016.pdf
[57] IPSOS https://www.ipsos.com/sites/default/files/ct/publication/documents/2018-05/unlocking_value_of_reputation-may_2018.pdf
[58] https://ec.europa.eu/docsroom/documents/40763
[59] https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf
[60] https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
[61] *The impact of IoT security labelling on consumer product choice and willingness to pay*, Shane D. Johnson, John M. Blythe, Matthew Manning, Gabriel T. W. Wong https://www.researchgate.net/publication/338813787_The_impact_of_IoT_security_labelling_on_consumer_product_choice_and_willingness_to_pay/link/5e6121c0299bf182deed36ed/download
[62] https://ec.europa.eu/docsroom/documents/40763

improved functionality, performance and security and pay 20-40% more for it compared with a cheaper brand. Alternatively, they may be willing to pay a smaller premium if the same product were to have its security enhanced (the 10% to 20% estimate mentioned above). Whilst it is difficult to estimate the willingness to pay precisely, this shows that consumers are indeed looking for more secure products.

In conclusion, the connection of equipment to a network can produce privacy risks, risks of fraud and risks to the network itself (e.g. misuse) that need to be addressed.

2.2. 2.2. What are the problem drivers?

Several studies and reports (from OECD, MS and consumers, see footnotes 8, 9, 16, 17, 19) identify that there is a lack of security features in the equipment and that MS do not have a harmonised legislative tool to remove insecure equipment from the EU market. The growth of internet-connected and/or wearable radio equipment will likely provide numerous benefits and business opportunities. However, there are associated risks which are inherent to this kind of connectivity. These risks arise from unauthorised access to radio equipment and the network communications that the devices undertake with local routers and/or more widely with other organisations.

These risks can be mitigated through a "Security by Design and Default" principle. This approach seeks to make systems as free of vulnerabilities and impervious to attack as possible through basic security measures such as continuous testing, authentication safeguards and adherence to best programming practices. This approach ensures that some security aspects are an integral part of product development so that it is embedded into the device at the manufacturing stage prior to being placed on the market, and not dealt with retrospectively.

However, several studies highlighted that certain radio equipment lacks basic requirements, e.g. protecting privacy or minimising the risks of fraud or preventing harms to the networks. This lack of basic requirements does not only represent a risk *per se*, but also may not support effectively the policy objectives of other pieces of EU legislation (e.g. the GDPR).

A number of stakeholders, in particular associations of consumers and MS, believe that cyber risks have grown significantly in the past five years, since cybersecurity has not been addressed through market access regulation. In particular, MS can only rely on possible national acts to withdraw products that are not "secured by design" from the market and therefore there is a need for specific action to have a solid harmonised legal basis at EU level for this purpose. Low-quality, non-cyber secure products remain legally sold on the European single market. The problem had in their view been exacerbated by the trend towards smart and connected products. MS and consumers also reported that certain products may individually be perceived as "less risky", but the growing number of such devices connected to networks (conservatively estimated to be several hundred million, see next section) creates a "great risk".

When placing radio equipment on the market, manufacturers are best placed to know the technical characteristics that would ensure a specific level of security. Consumers or certain users have limited or no capacities to perform this analysis. As a consequence, there are limited disincentives for manufacturers to place insecure equipment on the market at low prices. This makes secure products that are more expensive seemingly less attractive to consumers and users. This may in turn induce manufacturers to also cut on security in order to remain competitive, leading to a downward spiral. Another problem driver is a lack of consumer awareness regarding security. While there are some consumers that care about security (and would be willing to pay more), other consumers might not care at all. Yet these consumers can inadvertently create

problems for others (e.g. by becoming part of a botnet carrying out DDOS attacks).

2.3. 2.3. How will the problem evolve?

Internet-connected and/or wearable radio equipment is growing exponentially as a result of simple products being transformed into smart products and connected to the internet for a variety of reasons, including greater efficiencies, convenience, additional functionality, as well as facilitating ease of monitoring, servicing and maintenance. This process has strong potential to foster economic growth and to address societal challenges as it is recognised as an enabler that will increase efficiency in a number of areas, including transport and logistics, health, and manufacturing. It is expected to assist in the optimisation of processes through advanced data analytics, and be the catalyst for new market segments.

In a previous study[63] radio equipment usage between 2015 and 2030 was forecast for different application categories and more than 30 types of devices. The numbers therein contained have been revisited and, through desk research and interviews with experts, forecasts and predictions have been updated. This has led to small changes in previous forecasts and to a reduction for the number of tablets sold, which are now expected to decrease in the future.

Figure 1 provides an overview of forecasts for the number of radio equipment devices that will be in use across five application categories between 2015 and 2030 in Member States[64]. Estimates suggest there were 1,097 million radio equipment devices in the Member States in 2015. This is estimated to rise to 7.43 billion by 2030. This represents a compound annual growth rate (CAGR) of 14.6 per cent. The largest application category is expected to be devices associated with smart homes; it is expected that 4.5 billion of these devices will be in use in 2030 in the EU. The second largest application category is expected to be wideband data transmission devices. This category largely concerns devices used on short range local area networks typically using RLANs (Radio Local Access Networks). It is expected that 2.18 billion of these radio devices will be in use in 2030 in the EU. These forecasts highlight the large number of radio equipment devices – 7.7 billion – that are forecasted to be in use by 2030. This translates into 29 radio devices per household in 2030[65].

According to an Ericsson[66] report of May 2020, *Service providers' revenues from existing business, mainly driven by connectivity, are expected to remain stagnant, […]. Therefore, they are exploring new opportunities in order to capture a larger share of the potential global ICT revenue enabled by 5G, of up to USD 700 billion[67] in 2030 across 10 industries.* This confirms the expected future trend to switch to 5G and connectivity. Taking into account the ratio between the global and the EU population (approximately 6%), a conservative estimate is that the revenues for ICT products sold in the EU will amount to at least EUR 36 billion in 10 years, only for 5G-related technologies. It is then rather clear that there is a progressive

[63] Tech4i2. 2016. Identification of the market for radio equipment operating in licence-exempt frequency bands to assess medium and long-term spectrum usage densities. SMART 2014/0012. https://publications.europa.eu/en/publication-detail/-/publication/9994777b-2ba9-11e6-b616-01aa75ed71a1

[64] The study and data forecasts covered the EU28, even if the UK left the EU on 31st January, 2020.

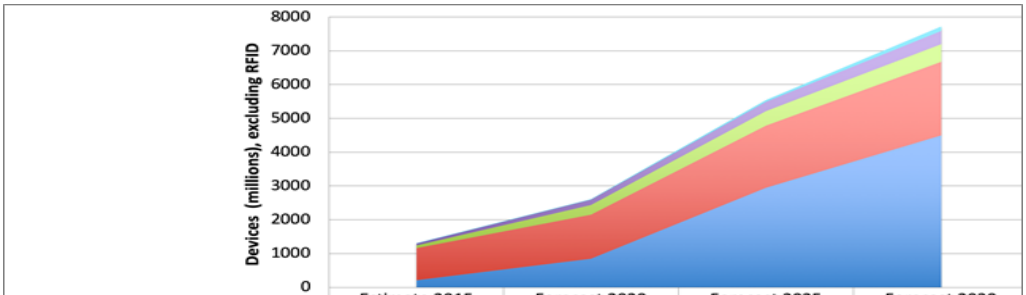
[65] Clearly devices will also be located in business and industrial premises, public buildings and outdoor locations, automotive vehicles and other locations. This figure, only calculating that all devices will be in households in 2030 (estimated as 258m households from linear extrapolation of Eurostat) is an overestimate, but it does serve to emphasis the enormous number of radio devices that are forecast in 2030.

[66] https://www.ericsson.com/assets/local/5g/documents/beyondmbb-5gforbusiness-2020.pdf

[67] approximately 600 billion EUR in October 2020

digitization of conventional goods and that attention has to be paid to ensure that the risks stemming from this increased connectivity are sufficiently mitigated. The large number of internet-connected and/or wearable radio equipment sold on the European single market emphasises the significance of the threats, vulnerabilities and the perceived impacts of device-level risks stemming from this increased interconnection.

Figure 1: Forecasts for radio equipment devices in use 2015 to 2030 (excluding RFID and medical devices)



	Estimate 2015	Forecast 2020	Forecast 2025	Forecast 2030
Transport & traffic telematics	3.0	11.9	45.2	132.0
Remote monitoring & wireless alarms	64.2	164.0	275.0	387.0
Audio/media wireless streaming	75.8	282.5	435.0	516.0
Wideband data transmission	948.5	1,304.4	1,836.0	2,184.0
Smart Homes (alarms and telecommand)	210.0	850.0	2,950.0	4,500.0

Source: Commission's contractor[68]

Whilst some industry manufacturing associations expressed the view that the nature of the risks has been exaggerated outside of smart toys, ICT and cybersecurity associations and cybersecurity testing houses mentioned that despite improved awareness among industry about the vulnerabilities, there are still too many products coming to the market that do not even have the most basic cybersecurity features integrated into smart products, making them vulnerable to hacking, attack and data thefts (see for instance the study in footnote 5).

With the increase in sales and use of conventional goods with a wireless functionality, which is an external factor (i.e. a development that contributes to the problems but will occur regardless of any possible EU action), the overall risks can only be expected to increase, unless they are compensated by an improved attention in manufacturing. Manufacturers putting insecure equipment on the market at low prices can appear more competitive and in turn also induce other manufacturers to cut on security, leading to a downward spiral. This requires to ensure at least a baseline mandatory degree of security of the equipment, to limit unsecure products from coming to the market.

2.4. 2.4. Impact of COVID-19

COVID-19 has already had a number of immediate implications on the EU engineering industries, such as supply chain dislocation in certain areas. However, it is likely to have ongoing economic impacts on the economy in the medium and longer-term[69], which are difficult to predict as the situation is constantly evolving. Consequently, it is difficult to form a comprehensive picture, both due to its ever-changing nature,

[68] https://ec.europa.eu/docsroom/documents/40763
[69] https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200610~a16c903e5c.en.html

and due to the absence of any reliable quantitative data from official sources. Indeed, even if official statistics were available, these would likely rapidly become out of date as the situation is fast-changing. The possible outcomes of the crisis are likely to differ significantly across different sectors of the economy. Regarding the general impact on GDP, the IMF expects European GDP across the EU-27 to decline by 7.5% in 2020. However, a rebound is possible as the economy recovers in 2021, but this is greatly dependent on many variables, which have such considerable uncertainty.

COVID-19 promoted the demand for more flexibility in production systems with an increased demand for augmented reality, cybersecurity, and big data applications. 3D printing could also provide solutions to help manufacturers overcome supply chain dislocation, for instance, when crucial components are unavailable due to lockdowns. Euromonitor, for example, forecasts 30% annual growth in the 3D printing market in the next few years, a trend it recognised had been accelerated by COVID-19.

The EU industries are already relatively digitalised, although they are behind US and Asian manufacturers in terms of the level of deployment of Industry 4.0 technologies. However, as in other sectors of the European economy, there is expected to be an increased pace of adoption of digitalisation both in terms of the adoption of digital manufacturing technologies, and in working practices due to COVID-19. According to a ZVEI survey[70], half of the companies participating in the survey intend to invest even more in digitization in the future than already planned due to the corona crisis.

Also from the consumers' side, the boost of online sales has been acknowledged. As early as March 2020, the European Parliament noted that[71] "*in South Korea, for instance, card and mobile payments grew 30 % between January and February 2020, as did innovation in contactless pickup and delivery services. As people stay at home more, they also download more online content and games for entertainment.*" In April 2020, the Commission has also urged the promotion of digital banking[72], while at the same time, remaining alert and continuing to fight financial crime, which is likely to increase in the context of the pandemic. The Commission has also launched consultations on (i) a retail payment strategy and a new digital finance strategy for the EU[73] in order to gather views on further developing European retail payments and digital finance so that citizens benefit from faster, cheaper and more efficient systems, while ensuring consumer protection and (ii) the revision of the NIS Directive to help the speedy digital transformation of our society following the sudden growth in demand for internet-based solutions. This means that increased attention has to be paid to ensure security of digital payments and protection from fraud, also on the equipment side.

More generally, COVID-19 has already had an impact in terms of accelerating the take-up of new forms of work organisation, such as remote working and the use of video conferencing, with more teleworking with own equipment (e.g. routers, sometimes their private laptops, etc) which may have not undergone a corporate strengthening of security. Once again, when sensitive meetings are to be organised remotely, it is paramount also to trust the devices which are used and the enforcement at the market access of products will support this trust.

[70] https://www.zvei.org/themen/corona/
[71] https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649341/EPRS_BRI(2020)649341_EN.pdf
[72] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_757
[73] https://ec.europa.eu/info/consultations/finance-2020-retail-payments-strategy_en

ENISA's report of October 2020[74] summarised that additional extraordinary measures had to be taken in urgency because of COVID-19: "*While working from home, cybersecurity specialists had to adapt existing defences to a new infrastructure paradigm, attempting to minimise the exposure to a variety of novel attacks where the entry points are employees' Internet-connected home and other smart devices. At the same time and under high-pressure, they had to implement solutions based on previously less trusted components, such as remote access through the public Internet, cloud services, unsecured video streaming services and mobile devices and apps. The necessary reaction to the COVID-19 pandemic to guarantee safety and at the same [time] reduce the impact on businesses, has pushed organisations to the limits of their ability to respond to changes. Furthermore, numerous modus operandi quickly adapted to the changing work patterns, cybersecurity professionals found themselves acting at the limits of their capacities*". This strengthens the need for timely actions under the available legal framework.

This need for a secure digital world has to be balanced against the call of engineering industry associations to maintain a stable regulatory framework, retaining a technology-neutral approach based on the NLF approach. The rationale is that the engineering industries are having to cope with not only major international competition, but also with the costs of the COVID-19 crisis. Therefore, the adoption of existing empowerments, such as delegated acts under the RED, can address the risks posed by radio equipment by adapting an existing framework and hence represents a viable trade-off between the needs of all actors.

3. 3. WHY SHOULD THE EU ACT?

3.1. 3.1. Legal basis

The RED is based on Article 114 of the TFEU. Certain RED requirements could be made applicable via delegated acts. More specifically, Articles 3(3)(d), 3(3)(e) and 3(3)(f) refer to network protection, safeguards to protect privacy and against fraud, respectively. This kind of protections objectives can be better achieved at EU level, rather than by the Member States alone, due to:

- The delegated powers conferred to the Commission by the RED, which would allow a harmonised framework for market access;
- The need for harmonised standards and interoperable solutions;
- The global nature of industrial value chains, as well as the activity of global competitors working across the markets.

Therefore, the EU can adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, the proposed measures will not go beyond what is necessary in order to achieve those objectives.

Any delegated act under Article 3(3) will make applicable the corresponding essential requirements for specific categories of radio equipment. It will also not require a co-decision process, as the co-legislators have already agreed to delegate specific empowerments to the Commission.

[74] https://www.enisa.europa.eu/publications/year-in-review

The RED is a new approach legislation, where only essential requirements are defined. Manufacturers are requested to demonstrate how the technical solutions in their products comply with the law.

3.2. 3.2. Subsidiarity: Necessity of EU action

EU intervention in this area is a common interest. As outlined above, the EU needs to make sure that products placed on the EU market support the trust in the technological transformation.

The technology to improve the security of connected and wearable products is available, and needs to be timely implemented and widely deployed so that the policy objectives of the Union can be reached. The scale and cross-border dimension on data privacy, frauds and network protection requires EU action. This can be widely identified in the reports from private, national and international Organisations described before.

Finally, national schemes are being discussed also for market access of products. It is consequently necessary to prevent the fragmentation of the Internal Market for aspects that can be regulated under the EU law.

For the specific case, the regulatory options considered in this Impact Assessment have built on existing delegated empowerments that the co-legislators had already introduced in the RED.

3.3. 3.3. Subsidiarity: Added value of EU action

Although legislation is already applicable to connected equipment, see Annex 6, the absence of enforcing measures when products are placed on the market does not make it possible to verify that products placed on the EU market contain appropriate safeguards or features to minimise the risks relating to frauds, violation of privacy or misuse of the networks. It is also not possible to recall them under EU law or impose corrective measures on manufacturers. While in a few cases, certain national criminal laws could be used to recall insecure products, this is not the case in all Member States. The policy objectives laid down in the mentioned pieces of EU law are then severely impacted. The *status quo* has likewise implicit quantifiable and non-quantifiable indirect (or implicit) costs which are expected to increase together with the increased use of interconnected products. A prompt response is therefore needed.

A regulatory action at the EU level, allowing market enforcement at the national level according to the NLF principles, will consequently fit a coherent implementation of the EU law, supporting the development of the Internal and Digital Single Markets and providing legal certainty for both manufacturers and consumers. In particular, it would allow to (i) verify *ex-ante* that equipment placed on the EU market is fit for the protection of the personal data and privacy, the protection from fraud and the protection of the networks and (ii) keep the current framework and conformity assessment procedures for placing radio equipment on the market. The EU is already contributing to voluntary schemes (e.g. by means of the Cybersecurity Act or codes of conduct under the GDPR) to ensure increased security. Based on this experience, the RED would request that certain related requirements are enforceable across the entire Union as a mandatory market access condition.

Manufacturers, who diligently addressed security risks in their products, would see their efforts rewarded against manufacturers who paid so far little attention to these risks. In this sense, an EU regulatory action will also establish a level-playing field for the equipment in scope, harmonising the requirements that are to

be demonstrated across the Union for market access, hence ensuring a common level of protection on the aspects in Articles 3(3)(d/e/f).

Also for these reasons, this initiative could improve the consistent implementation and application of the existing legislation in all Member States increasing predictability and legal certainty for all parties concerned.

4. 4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. 4.1. General objectives

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 (see Annex 6). This initiative should then allow on the EU market only the radio equipment which is sufficiently secure. The radio equipment presenting most risks would be covered.

4.2. 4.2. Specific objectives

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 which 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.

A graphical illustration of the intervention logic is contained in the form of a problem tree in the following page (Figure 2).

5. 5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

The different policy options include a status quo option, non-regulatory and regulatory options. The latter ones have been built on the existing empowerments in the legislation, namely delegated acts pursuant Article 3(3) of the RED. The focus on delegated acts under RED, in the context of the regulatory option, is explained mainly by the urgency to act. The Commission was asked by several Member States and stakeholders to act urgently upon those empowerments, existing since 2014, given that they were deemed to be sufficient to cover most of the risks in most of the concerned products, hence allowing a timely response.

The assessment of policy options has taken into consideration the extent to which the different policy options could achieve the policy and regulatory objectives set out above and in the Commission's inception impact assessment[75]. Different consultations of the TCAM Working Group, now Expert Group on Radio Equipment, took place to verify the extent to which the policy options could respond to the stakeholders' and the MS inputs. The options are outlined in the following box (table 1).

[75] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-6426936_en

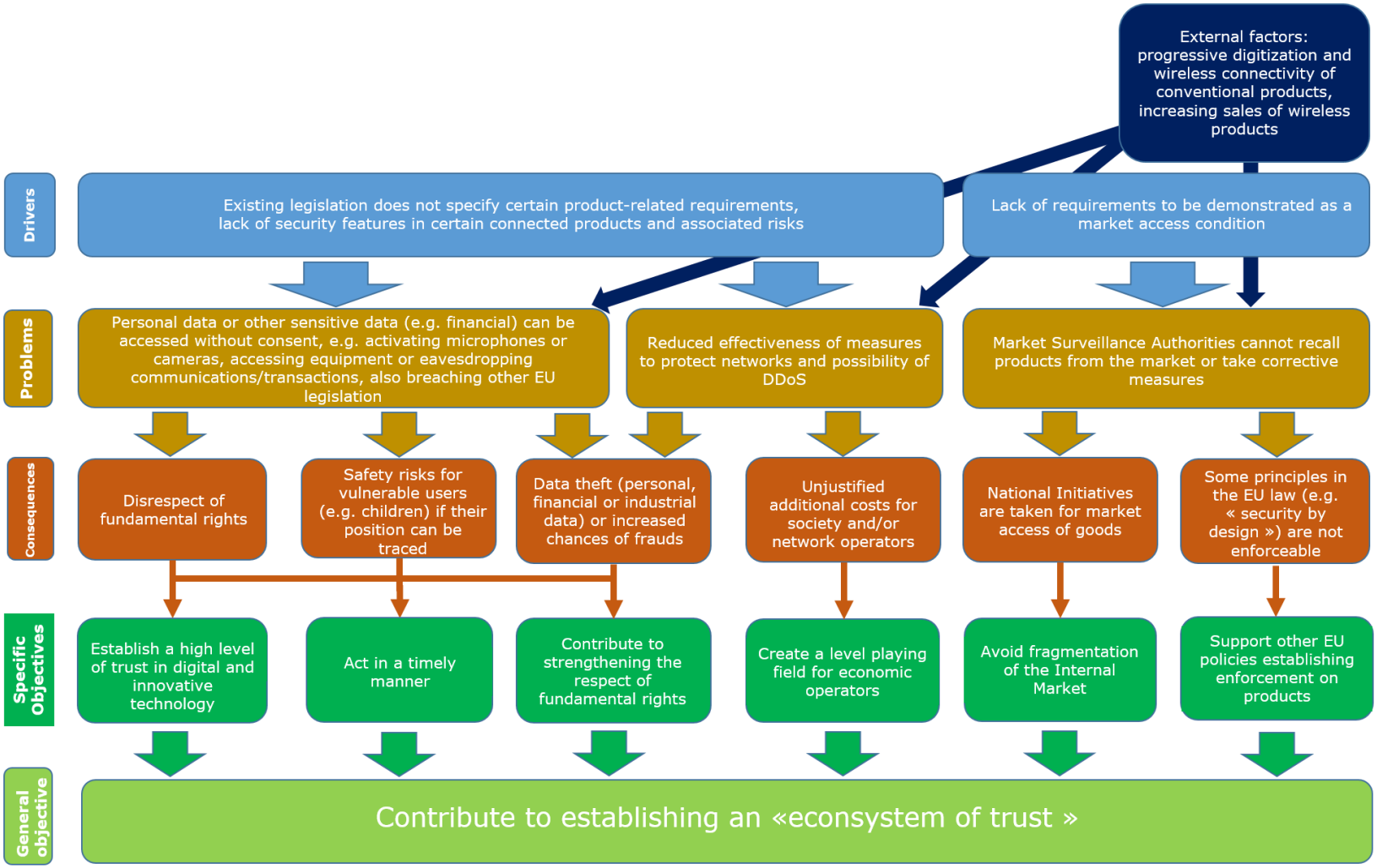


Figure 2: Intervention logic

Table 1: Description of policy options

Option	Description
Option 0 - Baseline scenario based on existing EU legislation.	A situation in which economic operators follow requirements in existing EU legislation (e.g. GDPR, e-Privacy Directive, NIS, Cybersecurity Act, etc). No specific requirements at product level for radio equipment.
Option 1 – Voluntary approach	A situation in which equipment manufacturers implement voluntarily features to protect personal data, protection against fraud and to protect the network where the equipment operates. This voluntary approach can be pursued using codes of conducts that are developed by either (i) industry alone or (ii) industry and authorities also on the basis of policy objectives in related legislation (e.g. see Annex 6).
Option 2 - Adoption of a delegated act based on Article 3(3)(e).	• Internet-connected and/or wearable radio equipment would be required to incorporate safeguards to ensure that the personal data and privacy of users and subscribers are protected. • Baseline security requirements would have to be demonstrated as a condition of market access.
Option 3 - Adoption of a delegated act based on Article 3(3)(f).	• Internet-connected and/or wearable radio equipment would be required to incorporate certain features to ensure protection from fraud, and a tool to enhance certain cybersecurity aspects of these products. • Baseline security requirements would need to be demonstrated as a condition of market access.
Option 4 - Adoption of two delegated acts based on both Articles 3(3)(e) and 3(3)(f).	• The requirements in Options 2 and 3 would have to be demonstrated for the purposes of market access. • This would entail manufacturers demonstrating that baseline security requirements have been met to ensure safeguards in respect of 1) data protection and privacy and 2) protection from fraud as a condition of market access.
Option 5 - Adoption of three delegated acts based on Articles 3(3)(d), 3(3)(e) and 3(3)(f).	• The requirements in Options 4 would have to be demonstrated for the purposes of market access. An additional delegated act would strengthen the requirements to ensure that radio equipment neither harms the network to which it is connected, nor misuses its resources. • This would entail manufacturers demonstrating that baseline security requirements have been met to ensure safeguards in respect of 1) data protection and privacy, 2) protection from fraud and 3) avoidance of harm to the network where they operate, as a condition of market access.

5.1. 5.1. What is the baseline from which options are assessed?

Policy Option 0 is the current baseline. Under this policy option, the status quo will be preserved, i.e. manufacturers and other economic operators of internet-connected and/or wearable radio equipment will not be requested to demonstrate certain essential requirements for market access either relating to data protection and privacy, or protection from fraud, or protection of the networks. The existing EU legislation – see Annex 6 – would be applicable but with the limitations discussed above.

In this scenario, manufacturers and other economic operators of internet-connected and/or wearable radio equipment will be allowed to place their equipment on the market even if they could be considered insecure, e.g. they do not provide certain basic protection.

Under Option 0, consequently, users of internet-connected and/or wearable radio equipment, or the networks to which they are connected, face the risks presented in section 2. The expected increase in the number of connected wireless products in use over the next few years and in the data that will circulate in networks of these products can reasonably be expected to lead to an increase of the risks.

Although in certain cases (e.g. a privacy breaches), corrective measures can be taken ex post, which may serve as a deterrent, they will come only after an investigation of the incident. However, products cannot be removed from the market other than through recourse to national legislation, which may also be subject to different interpretation[76]. This means that there can still be a risk for the internal market's effectiveness as regards the free circulation of internet-connected and/or wearable radio equipment, since there are no legal enforcement powers stemming from EU legislation to remove products from the market.

Indeed, some MS have instead had to use different pieces of national legislation[77] to find alternative ways for removing insecure products from the market where a risk of device penetration or data breaches could occur, and/or where the manufacturer was found to have placed a product on the market which did not respect data protection and privacy rules. Not all Member States could invoke a similar law, showing *de facto* a fragmentation.

Some technical solutions are common and they can protect privacy, prevent fraud and ensure network protection. Examples can be simple, as for instance (i) the avoidance of default passwords to access the equipment and/or (ii) the use of cryptography to store user's data and access parameters. Both these techniques can mitigate the chances that third parties take control of the equipment, accessing the users' personal or financial data and/or using the equipment to launch DDoS attacks. However, they are not mandatory and not all manufacturers adopt them, with the result that many risks which could be mitigated in manufacturing are present when the equipment operates.

5.2. 5.2. Description of the policy options

Policy Option 1 relates to the possibility of adopting a voluntary approach to addressing the concerns of consumer associations and national authorities. Two sub-options could be possible, i.e.

- A fully industry-led process with the development and publication of good practices and industry codes of conduct relating to internet-connected and/or wearable radio equipment OR
- A voluntary adherence to non-mandatory initiatives, such as EU-level codes of conduct and/or the incorporation of non-mandatory elements from EU legislation. Examples can be voluntary

[76] In the case of the Cayla doll, national authorities and Market Surveillance Authorities found that they were unable to remove the product from the market, even though various security flaws and vulnerabilities had been exposed. Germany, for instance, therefore relied on a longstanding piece of legislation relating to preventing spying to remove the product from the market.

[77] e.g. Germany had to invoke a federal law against espionage devices to ban a connected toy which intentionally transferred recordings outside the EU, see the German Agency press release in https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html?nn=690686

certification schemes under the CSA, or voluntary codes of conduct developed under the GDPR.

The rationale for defining these two sub-options is that several stakeholders, in particular equipment manufacturers, stated that a voluntary approach would only be effective if supported by accompanying measures, such as awareness-raising among manufacturers and other economic operators, and among consumers regarding the importance of ensuring high levels of data protection and privacy and protection from fraud through the enhanced security of internet-connected and/or wearable radio equipment.

ENISA has for instance developed baseline security requirements for IoT products[78]. While the focus of the original guidance document was on the specific risks posed when connected products are installed in particular locations, such as in critical infrastructures, the general principles relating to cybersecurity in the design of connected products have wider applicability and relevance. The general principles relating to security by design and default provide a starting point from which more detailed technical solutions for connected products could be developed in the future. The guidance on baseline security requirements is relevant irrespective as to whether the approach to taking their implementation forward were to be through an industry-led voluntary approach, or through a regulatory approach.

However, whilst codes of practice and other voluntary approaches to promote improved consumer IoT security may help in changing the behaviour of IoT device manufacturers over time, manufacturers of cheap equipment falling short of the expectations have limited or no incentives to introduce certain necessary improvements in the design of their products, as explained above in the problem definition section.

Under Policy Options 2, 3 and 4, either one or both of the delegated acts in the RED under Article 3(3)(e) and Article 3(3)(f) would be activated. Any delegated act under Article 3(3) will make applicable the corresponding essential requirements for specific categories of radio equipment. Mandatory requirements would be then introduced for manufacturers to ensure that their products are secure in relation to ensuring safeguards for data protection and privacy, for protection from fraud and/or protection of the networks. While each the options in principle addresses all problems, each of them has a different focus. There are common technical solutions that may be applied for instance to deal with privacy issues that also have a positive effect on fraud prevention. The precise technical solutions are to be established via harmonised standards under options 2-4, so it is not possible at this stage to present a thorough analysis of the extent to which each option addresses each problem. Yet, all options are likely to have a positive impact on each problem but to a different degree.

Policy Option 2 would consist of a delegated act under Article 3(3)(e) of the RED, and thus focus on the protection of privacy and personal data.

Policy Option 3 would be a delegated act under Article 3(3)(f) of the RED, focusing on the protection against fraud.

Policy Option 4 would be a combination of options 2 and 3.

Policy Option 5 stems from option 4 but includes the requirement that equipment should not harm the network. This addition was suggested by MS and stakeholders after the initial Inception Impact Assessment

[78] See: 1) ENISA (2018) *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot and 2) ENISA (2017) *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

as it was considered a needed and a logic complement to Option 4, based on the existing empowerments in the RED. The progressive requests of the Council to protect certain networks (e.g. 5G) can further explain this late addition. Finally, being certain technical solution in common, the inclusion of the protection of the network was assumed to potentially improve the benefits of the initiative, at reduced costs.

These options build on the essential requirements for whose adoption the European Commission has already been empowered by the co-legislators. Whilst the adoption of delegated acts would require manufacturers of certain categories of radio equipment, duly specified in the delegated acts themselves, to demonstrate new essential requirements as a market access condition, the rest of the provisions of the RED will remain applicable. Manufacturers, Authorities and other stakeholders can use the existing practices, Expert Groups, Committees, etc. These options would require minimum baseline security requirements to be implemented alongside existing applicable EU regulations.

Policy Option 5 builds on option 4, adding the protection of the networks as an additional policy objective to pursue. This option stems from a political request of the Member States in both the Council[79] and in the Expert Group on Radio Equipment, urging to take actions to enhance the resilience of radio equipment which will be connected to networks, specifically 5G networks, these being vital infrastructures in support of the economy. This request arrived after the data collection exercise and aims to complement the existing national work on the infrastructures. The Member States considered Article 3(3)(d) a needed complement to Article 3(3)(e) and 3(3)(f). At the technical level, the request originates from the complementarity of many technical solutions that, once applied to protect personal data and against fraud, also can protect the network, which has been confirmed also by relevant Committees in the European Standardisation Organisations.

The RED is aligned to the NLF. Consequently, for all regulatory options from 2 to 5, following the procedures in the Standardization Regulation 1025/2012, the Commission would request European Standardisation Organisations (ESOs) to produce harmonised standards so to allow manufacturers to benefit from the presumption of conformity, in line with Articles 16 and 17(3) of the RED. The request would also contain a reference to appropriate pieces of EU law, see Annex 6, whose implementation would benefit from ensuring that radio equipment demonstrates new essential requirements for the purposes of market access.

5.3. 5.3. Discarded options

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. In addition, at the time of the revision of other sectoral legislation, e.g. on medical

[79] see section 2.1.3

devices[80], this option was also not considered, given the urgency to address risks in those products. The sectoral legislation was then favourite as the evidence of risks is stronger. Consequently, although there are still residual risks and products that may need to be addressed by a complementary horizontal initiative, this option has been discarded, favouring the timely adoption of a delegated regulation (options 2 to 5), which could effectively address in the short term the most urgently perceived security risks in a broad range of products. The policy option of establishing a mandatory cybersecurity framework was considered viable in the medium-long term and not retained for this initiative. This approach is fully in line with the recent Council's conclusion (footnote 13) which while acknowledging the need "*to address in short-term ICT cybersecurity aspects in relevant legal acts, for example the New Legislative Framework (NLF) including the within Directive 2014/53/EU (Radio Equipment Directive)*", underlines "*the importance of assessing the need for horizontal legislation, also specifying the necessary conditions for the placement on the market, in the long-term to address all relevant aspects of cybersecurity of connected devices, such as availability, integrity and confidentiality*."

- 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. When the act was adopted as a voluntary piece of legislation, it was considered covered under the industrial voluntary approaches in section 6.1.
- 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. In addition, a stand-alone option for Article 3(3)(d) would have ignored the documented risks (see footnotes 8, 9, 16, 17, 19) that triggered the initiative and would not have allowed to meet some of the specific objectives (in particular the risks to privacy and of fraud of specific radio equipment) and hence would have mitigated the risks only partially.

6. 6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

Economic, social and environmental impacts were considered in assessing the policy options. In more detail, it was sought to have a quantitative analysis, wherever possible, of the following aspects.

Considered economic impacts included:

1) Administrative costs for manufacturers and economic operators;
2) Substantive compliance costs for manufacturers and economic operators;
3) Enforcement costs for Authorities;
4) Other direct costs, i.e.:

[80] 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. 1–175*

a) For professionals and industry, costs directly attributable to data breaches and DDoS and post-breach activities to manage the fallout e.g. informing customers about data[81] and information compromised, restoring network integrity, auditing with IT security specialists to rectify the problem, strengthen security and/or possible related litigation costs/liability matters;
b) For citizens, (i) money lost due to financial fraud, (ii) identity theft and (iii) the consequent resources that have to be spent to remediate possible matters (e.g. changing credentials, dealing with banks or credit card providers, etc). Apart from the one in (i), the other two costs are mostly not quantifiable.

5) Indirect costs/benefits:
   a) Reputational damage, with related loss of customers and value for investors;
   b) Users' trust in the Digital Single Market and related sales and costs of internet-connected and/or wearable radio equipment;
6) Improved functioning of the Internal Market by ensuring that a level playing field is maintained without the emergence of national divergent legislation;
7) Competitiveness of EU industry in the digital economy.

Limitations of the analysis

In all considered policy options there are risks of fines issued by data protection authorities[82] due to the non-compliance of the equipment with regulatory requirements under the GDPR. The fines are significant, up to EUR 20 million, or up to 4% of the annual worldwide turnover of the preceding financial year, whichever may be greater. These costs affect the data controller, who is often not the manufacturer of the equipment. For the purposes of this impact assessment, it cannot be excluded that in some cases the protection of the equipment may have helped mitigating the privacy risks, avoiding the fines. The obligation for manufacturers of ensuring "security by design" of the equipment, demonstrated as a market access condition may in turn facilitate compliance efforts for the controller of the data under the GDPR (by ensuring a certain baseline of security features in the equipment). In the absence of precise information on the extent of fines which were due to lack of safeguards in the equipment, costs generated by fines under the GDPR are herein not reported.

With respect to compliance costs of the different options, in general, economic operators found it hard to estimate them, in the absence of the text of the delegated acts and the related specifications to comply with. Moreover, they assumed that different costs could be faced depending on whether future harmonised technical standards would contain common minimum generic requirements for all categories of internet-connected and/or wearable radio equipment, or whether these would be more product-specific. It was also unclear in their view how far future harmonised technical standards are likely to be based on existing technical standards, such as international standards and industry standards. In such case, it was also seen as difficult to differentiate between the costs of either Articles 3(3)(e) or 3(3)(f) as most technical standards focus on strengthening cybersecurity in general, by preventing unauthorised penetration[83]. Some further responses from the economic operators highlighted that it is still uncertain whether the same test would ensure compliance with other EU legislation and the RED. Examples in this regard are (i) data protection by

[81] In case of breaches of personal data, the obligation to inform those affected about breaches likely to result in a high risk to the rights and freedoms of natural persons under GDPR already applies
[82] https://edpb.europa.eu/news/national-news/2019_en
[83] The joint applicability of certain technical specifications to Articles 3(3)(d), 3(3)(e) or 3(3)(f) has been confirmed also in some exchanges with the ESOs

design and default (which includes "security by design" aspects) under the GDPR and/or (ii) voluntary product-specific CSA certification scheme. It was possible to partially overcome this challenge, by:

- Undertaking an assessment of technical solutions that are already available;
- Reviewing good practice guidance produced by ENISA setting out minimum baseline security requirements on specific equipment, i.e. consumer IoT security. These provide an indication as to what baseline security requirements might look like, and have been factored into the impacts;
- Gathering selected examples of compliance costs through product case studies;
- Limiting the assessment to the incremental costs. In fact, manufacturers of internet-connected and/or wearable radio equipment are already under the obligation to incorporate data protection by design and default into their business processes as part of GDPR compliance. A regulatory initiative under the RED will only make enforceable this obligation, hence only the additional costs are to be considered in the net costs.

Considered social impacts[84] were:

- General resilience against criminal activities, including avoidance of certain indirect (e.g. personal safety) risks that consumers and citizens may suffer[85];
- Protection of fundamental rights (e.g. to privacy).

Both these impacts include unnegotiable rights and can be related to non-financial aspects, e.g. anxiety, stress or physical harm, as a result of an incident. The inherent subjectivity makes it impossible to quantify possible negative social impacts on the individuals. At the general and aggregated level, however, these social impacts are reflected into the trust in the new technologies and the interconnection of conventional goods which on the contrary could be estimated – see point 5.b.

A general remark on environmental benefits is that, compared to economic and social benefits, there was less stakeholder feedback. Some large manufacturers commented that there remain some low-quality, cheap and insecure internet-connected radio equipment and/or wearable radio equipment on the European market which may already not meet minimum benchmarks. In their view, removing such products from the market could translate into European consumers purchasing better quality and could help to reduce purchases of low-quality equipment with a shorter product lifecycle. This in turn should help contributing to the circular economy and sustainability by lengthening the average lifespan of the use of such products, reducing unnecessary use of raw materials and the amount of electronic waste. This reasoning applies to all regulatory options. However it was neither confirmed by other stakeholders, nor could be substantiated in more detail. As a consequence, although acknowledging some reasonable elements in it, it is herein assumed that this initiative will not have environmental aspects and for brevity these will be omitted in the following analysis.

6.1. 6.1. Policy Option 0 – baseline scenario

Under this option equipment manufacturers would need to comply with existing legislation, yet MS will not be able to enforce equipment at the moment of placing on the market. We refer to Sections 2.1 and 2.3 for an

[84] Consumers' trust in the DSM is already addressed under point 6 above

[85] An example is the possibility of communicate with children/vulnerable users or access their position with the intention of harming or abducting.

assessment of the costs and risks of non-action. The insufficient incentives for manufacturers to incorporate adequate security measures in their products, as described at the end of Section 2.2, will remain, despite the targeted consultation showing that the vast majority of the respondents identified risks, and that there is the possibility to mitigate them.

In the consultations, this *option* was supported by equipment manufacturers only, with Member States, Consumers' associations and information security industry strongly opposing it. A summary of the different stakeholder positions is contained in Annex 2.

6.2. 6.2. Policy Option 1 – voluntary approach

Under this option the participating equipment manufacturers would incur some substantive costs (although a large part may be business as usual costs if the ones participating are likely to be the more security-minded) while those not participating would not incur any additional costs. Authorities would not incur additional enforcement costs, but they would also not have corrective measures against insecure products.

As regards the other costs analysed above (costs of data breaches for industry and consumers, reputational costs, trust), it is noted that, as of the launch of the Inception Impact Assessment for this initiative, the Commission Services in charge have not received any commitment on the possible implementation of a voluntary approach. Moreover, in the discussions in the Expert Group on Radio Equipment or in the interviews with stakeholders, no information was provided by the represented associations of stakeholders on a possible scope, date of applicability and content of a possible voluntary approach and supporting stakeholders.

The application of a voluntary certification scheme under the CSA has been considered under this option, but no indications have been given on the willingness of manufacturers to take it up, when available. In any case, a voluntary labelling scheme would not fully address the identified risks, e.g. with respect to enforcement.

It is consequently not possible to assess the impact of any concrete voluntary initiatives. In particular, it is not possible to estimate whether their benefits would compensate for the costs of non-action described in the previous Section. Finally, a voluntary initiative might cover only part of the manufacturers while others may prefer to avoid additional costs. It is likely that the producers of the most problematic cheap equipment would not join a voluntary initiative as this would not be in line with their business strategy, which would seriously hamper the effectiveness of voluntary action. This would be detrimental for the establishment of consumer trust and a level playing field among manufacturers.

It is also not possible to estimate how the Internal Market can be preserved, e.g. whether the level of voluntary commitment would be sufficient to avoid national legislation.

6.3. 6.3. Policy Option 2 – Article 3(3)(e), focus on protection of privacy and personal data

This option foresees to activate Article 3(3)(e) of the RED, with mandatory requirements to ensure that internet-connected and/or wearable radio equipment integrates safeguards to ensure that the personal data and privacy of users are protected.

Compared to the baseline scenario, there will be costs for manufacturers of equipment and economic operators in general. Most of the economic operators saw little differences in these costs under Policy Option 2, 3 or 4 and replied under the assumption that Option 4 would be adopted. Findings are consequently

presented in Section 6.5. In more general terms, existing technical solutions related to the protection of privacy problems also relate to the protection of the network and the protection against fraud. An example is reported in section 6.6, based on an existing European (and international) standard.

Feedback was received from economic operators through the targeted consultation about the administrative costs. It should be noted that whilst 56 responses were received to this survey, the questions on administrative costs and burdens were answered only by economic operators, and the survey cohort is therefore 28. This is a relatively low number, but the survey responses have been cross-checked against the feedback from interviews with manufacturers carried out as part of the product case studies. Economic operators were almost unanimous in stating that there would be additional administrative costs related to new regulatory requirements on data protection and privacy.

With regards to the "Business as Usual" costs, the related obligations under the RED will be applicable in any case. The extra administrative costs will be on (i) familiarising with the new requirements, (ii) updating the Declaration of conformity, (iii) the technical file and (iv) information to the users. No quantitative information was provided in this respect, although in Section 6.5 is reported a synoptic – figure 5 – of the perceived severity of the costs in case of adoption of both Articles 3(3)(e) and 3(3)(f). It is not possible to break it down to the individual acts. Economic operators were mostly concerned by the impact on testing costs. The particular lack of harmonised standards was flagged as a key factor, which could raise or remove costs significantly, also for Small and Medium Enterprises (SMEs). This severity also stems clearly from the above-mentioned synoptic figure and, quantitatively has been provided in aggregate for Articles 3(3)(e) and 3(3)(f), hence it is reported Section 6.5.

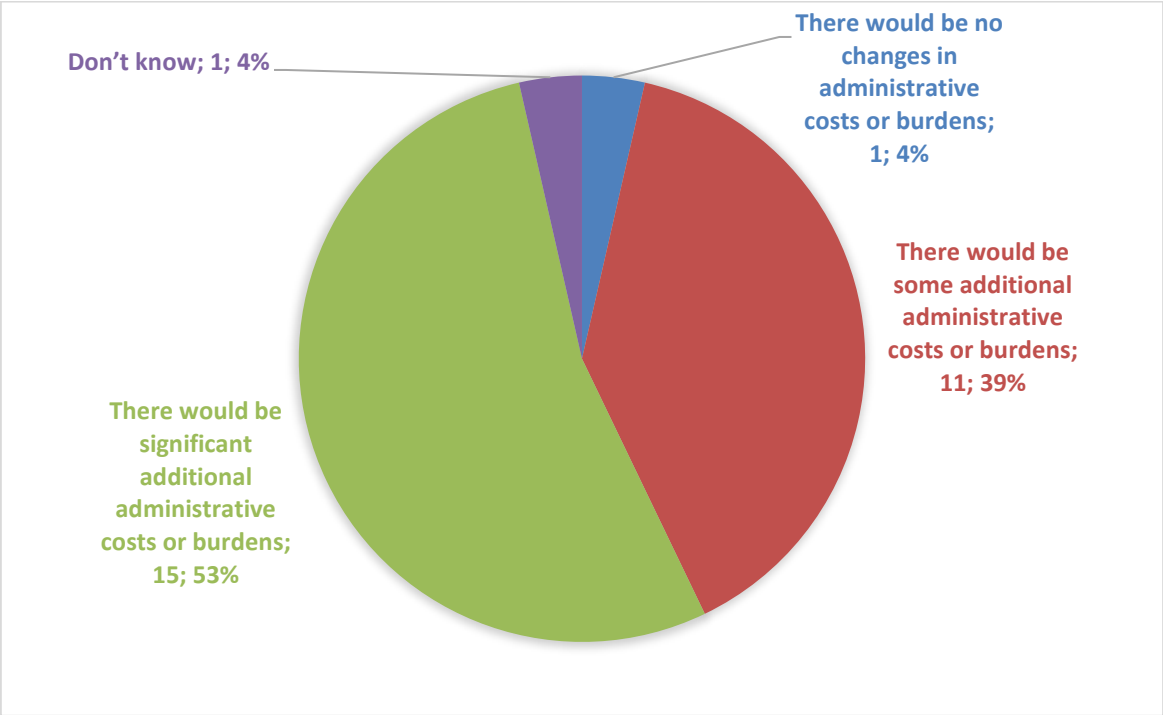
The costs of internal testing and third-party conformity assessment are considered one of the major areas of costs associated with demonstrating compliance with the essential requirements. In some cases, also other substantive compliance costs (e.g. costs of redesigning products) were reported as a source of concern. However, it was not possible to collect the information on the extra costs that will be caused by the introduction of regulatory requirements under the RED in addition to the costs that manufacturers have already incurred to comply with the GDPR.

In any case, in order to mitigate these costs, the Commission services have already started a discussion with the ESOs, asking in particular a mapping of potentially applicable solutions in order to develop an understanding of (i) the risks that can be covered already and (ii) the gaps that may require additional efforts to ensure a smooth functioning of the Internal Market of radio equipment. A working draft document[86] has been distributed to and discussed in the Expert Group on Radio Equipment for comments and general awareness. Many technical solutions identified in this mapping are in common to the GDPR and/or the CSA. Whilst the GDPR does not impose technical solutions for market access, the CSA schemes are voluntary and manufacturers have always the discretion to apply harmonised standards, the Commission services will spend increased attention to ensure coherency between the implementation of these (and other possibly applicable) pieces of EU legislation. As mentioned, whilst these pieces of legislation address different aspects of the same problems, risks of conflicting implementation are to be avoided. This exercise can also be anticipated by the industrial stakeholders themselves, who, sitting in several standardization fora, can

[86] https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/3d3719b9-b0ff-4764-ae7f-d940e3a212ae/details

develop standards and technical solutions bearing in mind the related applicable frameworks. If a comparison can be made with other essential requirements of the Directive, for Article 3(2) – concerning the efficient use of radio spectrum – 140 "unique" harmonised standards[87] have been produced and cited in the Official Journal of the European Union, with others in preparation. Nothing would prevent that the same approach is followed also for Article 3(3), with a consequent production of an appropriate number of harmonised standards which would address the risks of equipment according to the intended use in a proportional and effective manner.

Figure 3: Administrative burden of new regulatory requirements (data protection & privacy)



Source: targeted consultation, online survey

Market Surveillance Authorities (MSAs) stated their estimated costs for enforcing the new requirements would be in the order of EUR 5,000 – 10,000 for each type of simple equipment, and up to EUR 20,000 for each type of more complex equipment, per equipment type. Overall, these costs were found to be proportionate to the benefits, with a high level of "Business as Usual" (BaU) costs[88] of some 60-70%.

In this scenario, the rest of the costs and risks described in option 0 will be mitigated, as a function of the technical solution(s) employed in manufacturing. However, the costs of financial frauds and the costs incurring from a misuse of the network will not be prevented, unless these technical solutions can be used for these purposes (e.g. encryption). It will not be possible to ensure a more coherent approach to the implementation of the non-cash payment Directive.

[87] i.e. without counting multiple versions or revisions
[88] costs relating to the normal conduct of business regardless of special circumstances, which may pose possible negative or positive impacts. http://www.businessdictionary.com/definition/business-as-usual.html

No stakeholder preferred this option.

6.4. 6.4. Policy Option 3 – Article 3(3)(f), focus on protection from fraud

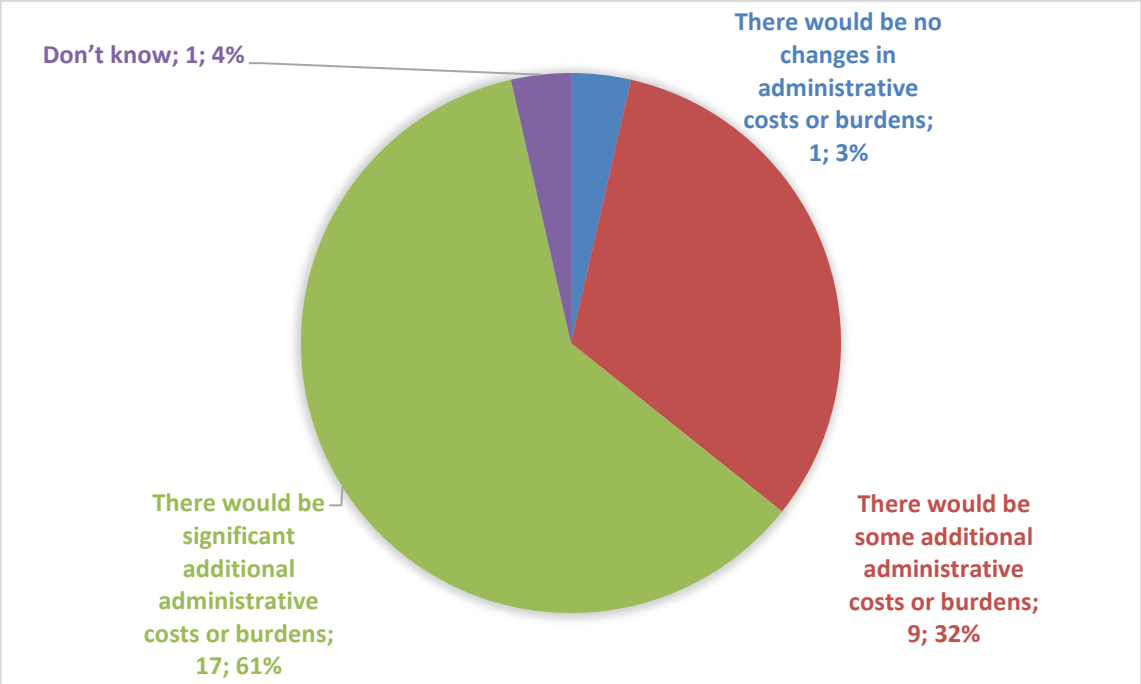
Under this option Article 3(3)(f) of the RED will be made applicable to "internet-connected and/or wearable radio equipment", so that equipment integrates safeguards to ensure protection from fraud.

This scenario is similar to that in Option 2, but it will not be possible to enforce the presence of features aiming to protect privacy and personal data as a condition for market access. On the contrary, a more coherent approach to the implementation of the non-cash payment Directive will be ensured, i.e. this initiative will ensure that equipment contains technical features so to minimise the risks of non-cash payment and hence support the general policy objectives laid down in that piece of EU legislation.

As most of the economic operators saw little differences in these costs under Policy Option 2, 3 or 4, the same considerations on the costs can be applied. Also in this case, certain existing technical solutions related to the protection against frauds can benefit the protection of the network or the protection of privacy. It is yet to be noted that economic operators are in this case slightly more concerned about the costs, as there is a more widespread knowledge on the GDPR than on fraud-related legislation. In any case, the mitigation of costs through a standardization request would be deployed. Through this exercise the manufacturers sitting in the ESOs will work on the production of harmonised standards in a dialogue with Authorities and other stakeholders, striking a balance between performance and costs, on the basis of what is technologically feasible. The reference objectives under this option will not be those of the GDPR but of fraud-related legislation. For the specific case of payments fraud the necessary steps to prevent it were better understood and acknowledged in terms of technical solutions. As in the previous case, benefits for network security and a coherent approach with the NIS will not be possible, unless some technical solutions are in common (e.g. encryption).

Similarly to Option 2, no stakeholder preferred this option.

Figure 4: Administrative burden of new regulatory requirements (fraud)



Source: targeted consultation, online survey

6.5. 6.5. Policy Option 4 – Article 3(3)(e) and 3(3)(f), focus on protection of privacy and against fraud

Stakeholder feedback on costs and cost drivers has been gathered through the interview programme and online surveys. The evidence base draws on the feedback from 28 economic operators (often large firms) that responded to the targeted consultation, interview feedback from EU industry associations representing producers of internet-connected radio equipment, and interview feedback with circa 25 interviewees from a further 15 manufacturers carried out through the 6 product case studies[89]. The synoptic in Figure 5 shows how costs were perceived by manufacturers or economic operators.

External, third-party product testing and certification to ensure compliance were regarded as the greatest area of cost (68% stated that these would be high), which was confirmed in the interview programme through discussions with industry stakeholders and individual manufacturers.

Testing costs were provided as in table 2. They typically refer to third-party testing costs, unless specific additional information is therein given. Clustering the provided data, third-party testing costs for each model being produced are likely to be in the order of:

- EUR 5.000 – 15.000 for "simple" products[90];
- EUR 20.000 – 30.000 for more "complex" products[91]; and

[89] https://ec.europa.eu/docsroom/documents/40763 - Annex 8
[90] i.e. products with a short and limited value chain in terms of hardware and software manufacturers

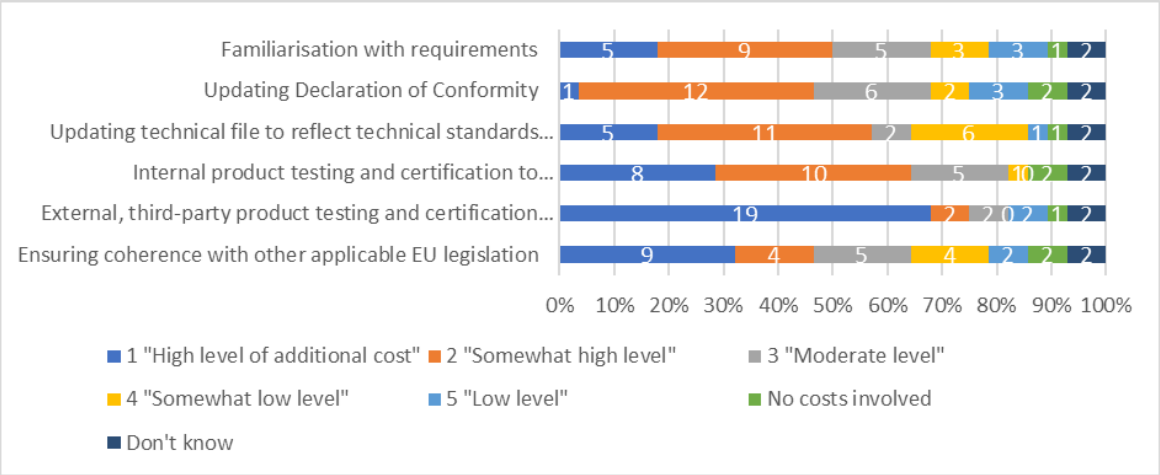
- EUR 50.000 or more for heavily software-dependent products.

However, it is worth noting (see table 2) that some costs are covered in the BaU and that the BaU is much higher for complex products than for simple products. Specific case studies on simple products estimated that in this scenario:

- Costs for connected lawnmowers manufacturers are expected to grow approximately by EUR 3-13 per piece of equipment, i.e. in the order of 0.5-4% of the retail price;

- Costs for routers manufacturers are expected to grow approximately by EUR 0.35 per piece of equipment, i.e. below 1% of the retail price.

Figure 5: Examples of costs estimated by manufacturers or economic operators



Source: targeted consultation, online survey

Details are reported in Annex 7.

The data summarised above and the BaU costs in table 2 are overall in line with the estimates of MSAs, which are the same as for Article 3(3)(e).

A specific concern among large firms and multinationals was that the costs of external testing and certification could risk being duplicated across different regulatory jurisdictions if EU rules diverge from international ones. It was noted that testing costs are similar across these countries and regions, but there would be additional, cumulative costs if the regulations diverge too much, as technical documentation would need to be customised for each jurisdiction and retesting could be required. As pointed out in the previous sections, the Commission services are already monitoring the situation. It is not unusual that international standards can be transposed into harmonised standards and provide presumption of conformity for the purposes of accessing the EU market. In some cases, however, the ESOs modify the international standard specifying better some requirements (e.g. through "common modifications" in CEN, *Comité Européen de Normalisation*, and CENELEC, *Comité Européen de Normalisation ÉLECtrotechnique*). Whilst in non-EU countries any potential unspecific requirement would be checked in the type-approval assessment procedure,

[91] i.e. products with a longer and more diverse value chain in terms of hardware and software manufacturers

in the EU the harmonised standards would guarantee direct market access. It is consequently important that harmonised standards ensure the same level of protection and the same level of legal certainty for manufacturers[92] as a type-approval regime. The industry sitting in the international standardization fora can ensure the drafting of international standards such that they can be timely and smoothly transposed into EU harmonised standards. In turn, this would maintain the success of the NLF, which has struck a fair balance between all interests at stake, in particular guaranteeing flexible and non-burdensome market access conditions for manufacturers and an adequate level of safety and performance for consumers.

As regards SMEs, two other main aspects were flagged, although in a qualitative manner:

- There can be SMEs of internet-connected and/or wearable radio equipment with a large product catalogue, but small volume productions. Actually some industry associations noted that large-scale manufacturers producing in high volume were better placed to absorb testing costs as the total costs can be spread across many units, so testing costs per unit are low. Conversely, producers of low-volume and/ or specialist internet-connected radio equipment may find it challenging to cover the costs as unit cost testing is high. Smart alarms were cited as an example of a sector where SMEs can produce different models in low volume;

- It was also reported that many (but not all) SMEs lack awareness and knowledge about cybersecurity in general, including security measures to ensure adequate data protection and fraud. It may therefore be relatively costly for them to gather the appropriate competences, reengineer some of their products, or part thereof, and implement appropriate technical solutions, such as encryption and user-authentication, into their products.

With respect to the protection of privacy, substantive costs that SMEs will have to bear were reported. In more general terms, 78% of the respondents to the targeted consultation believed that there would be substantive compliance costs. Of those, three-quarters believed that the research and development costs would be high to redesign chipsets or components and to design compliant products. However, some of them reported that the extent of substantive compliance costs would depend on whether certain existing security features already incorporated into internet-connected radio equipment or wearable radio equipment would be sufficient to meet any new legal requirements.

Concerning compliance costs, especially for SMEs, it may be worth noting that:

- The RED Guide[93] already allows manufacturers carrying out their assessment on the product, to use assessments performed previously (by other companies) for components or parts. This distributes the tests and the needed competences through the value chain. A similar principle also applies to Notified Bodies who may have approved a specific part or component[94];

---

[92] e.g. in enforcement

[93] https://ec.europa.eu/docsroom/documents/33162

[94] Section 6.2.1 of the RED Guide: "Where a notified body performs an examination of the technical documentation of an equipment that contains a radio part for which already a notified body EU type examination Certificate is available then the notified body may accept the results of that previous Examination without the need to repeat the assessment of that product part"

- Consequently, SMEs integrating components (e.g. wireless chipsets) from different suppliers can hence rely on the demonstrated security in the value chain and would be expected to have the capacities of preserving the demonstrated security when assembling different components. Most of SMEs in the sector integrate components. Most of the production of chipsets, integrated boards, radio modules is manufactured outside the EU. A scope which includes the value chain has the benefit to proportionally assign the needed compliance tests and hence the costs to the relevant manufacturers, limiting the burden on the assemblers;

Table 2: Examples of the costs of third-party testing for economic operators

Type of equipment	Estimated costs (and any notes)	BaU costs	BaU rationale	Days of testing
Simple internet-connected RE	Testing to check the product against minimum baseline security requirements. Minimum: circa EUR 5,000. More common testing costs: EUR 7,000 – 15,000	30%	Most producers undertake some kind of security testing (albeit internally).	1-10 days
Testing a niche, mono-functional product.	Between EUR 30,000 and EUR 40,000	30%	Most producers undertake some kind of security testing (albeit internally).	1 month
Simple and complex internet-connected radio equipment	EUR 3,000-5,000 to test a Bluetooth update	80%	Most producers already test Wi-Fi and Bluetooth updates and integrate in their products, though the duration they maintain software/ firmware updates post market placement varies.	2-3 days
Complex internet-connected radio equipment	EUR 20,000 - 25,000 for testing and conformity assessment. Security vulnerability assessment against a set of criteria.	60%	Many responsible manufacturers already carry out a risk assessment during the product development and testing process. This often includes a security vulnerability assessment.	10 -15 days
Complex internet-connected radio equipment (with extensive software)	Total costs, EUR 170,000. Internal costs 4 software engineers – EUR 60,000/ year X 6 months development cost = EUR 120,000. External costs EUR 50,000 lines for checking software code of more complex internet-connected radio equipment products. One quarter of the costs were direct compliance costs internally and three-quarters were external costs to procure code checkers. Note that distinguishing the costs between checking software and performance are difficult	80%	Many manufacturers pointed out that they already test products extensively for performance and functionality and in parallel for their security. Additional costs could arise from familiarisation with harmonised technical standards rather than using their own internal testing standards, given preference by many manufacturers to use EN standards once developed.	6 months internal testing 1 month (external testing only)
Routers	C.a. EUR 129,000 net for security, including a combination of internal software development and product testing and external validation testing. EUR 60,000 for internal testing costs and software development (security aspect only). EUR 69,000 lines for external testing of software. See case study for detailed disaggregation.	90%	High BaU as the manufacturer sells its product to the wholesale market (to telecoms providers and ISPs rather than directly to retail. Therefore, high-performance and security functionality is required even in the absence of legislation.	1 month
Wearable radio equipment	>EUR 35,700 Combination of internal and external testing costs.	Unknown	Estimation from a wide range of data from across the studies and interviews	1-2 months
Testing garden equipment	EUR 20,000 - 25,000 per product.	20%	According to an EU industry association, most gardening equipment products that are connected only have limited security features. Therefore, integrating any requirements e.g. for the chips and processors to be encrypted was viewed as involving (considerable) additional costs (see case study on gardening equipment).	1 month

Source: Commission's contractor

- All manufacturers of radio equipment or their components, including SMEs, should already have taken steps to ensure that their products can be used in a way that complies with the "security by design" principle in the GDPR. Article 3(3)(e) will request to demonstrate this security by design as a condition for market access. As will be illustrated in the next section, there is a strong correlation between Articles 3(3)(e) and 3(3)(f) – and also 3(3)(d) – so the awareness and capacities that are required to comply with Articles 3(3)(e) and 3(3)(f) together are less than the sum of the parts.

Box: Insight into the cost drivers of security in smart toys – uncertainties in quantification.

Examples were identified where products would need to be redesigned and/ or re-engineered if the delegated acts under option 4 were to be activated. The Cayla doll was cited by several stakeholders as an example of a product that would have to make substantive changes to ensure suitable security safeguards to protect users' personal data and privacy. But the costs involved were difficult to estimate, due to uncertainty as to what the new requirements might be, and whether the industry has already taken sufficient steps to strengthen the security of connected, smart toys.

Leading toy manufacturers interviewed and the industry representative association at European level pointed to significant changes having been made across the industry to strengthen product security. This was seen as having been driven partly by recent regulatory obligations under the GDPR having led to the better documentation of business processes relating to compliance, especially with Article 25 (data protection by design and default). A further driver was the importance of risk and reputational management, necessitating investment in security even in the absence of any additional regulatory requirements.
This suggests that if substantive costs were incurred, there may be high BaU costs, as leading toy manufacturers are already integrating data protection and privacy considerations as part of their broader approach to integrating security by design and default principles. The advantage of regulatory options would be to ensure that all manufacturers actually take similar actions preventing some manufacturers to adopt a lower level of security.

It is noted that Article 25 (data protection by design and default, including security by design) is already applicable to manufacturers if they are intending to collect personal data themselves as they will then fall under the GDPR as data controllers. Regarding coherence between the RED and the GDPR, as discussed before, the RED will have the added value of allowing enforcement at the moment of placing on the market. The costs of an initiative under Article 3(3)(e) are then expected to be already incurred in part, if not fully. It has already been noted that some technical solutions under Article 3(3)(e) can be applied also to Article 3(3)(f) – see the mini-case study in the box below. A further example is provided in the section 6.6, also including network security aspects in the picture. This partial overlapping of the technical solutions makes it possible that the costs of adopting Article 3(3)(e) and 3(3)(f) together are smaller than the sum of the individual costs of Options 2 and 3.

Box: The benefits and costs of encryption

Encryption can have number of benefits as regards protecting the unauthorised penetration of internet-connected radio equipment. It helps those using radio equipment products and devices to safely move to the cloud, which is essential given productivity and efficiency benefits in an industrial IoT context and the

growth of consumer IoT and increased data capacity needs. Encryption also helps manufacturers to address requirements relating to the prevention of fraud or protection of networks. For instance, the payments industry has guidelines to ensure the protection of cardholder data and encryption is an important dimension of security standards in use in Europe and globally. However, encryption can be costly.

Existing technical solutions: There are many encryption solutions available on the market, though not all of them may be implemented in specific equipment, e.g. the one with limited processing power[95].

The costs of encryption: There were concerns that higher compliance costs may be incurred if the encryption requirements are set at too high a level, especially for internet-connected and/or wearable radio equipment that are sold at a relatively low price.

It was exceptionally difficult to obtain actual costs data. However, some secondary data was available. A 2012 report on the *"Total Cost of Ownership for Full Disk Encryption"* [96] was based on a survey of 1,335 IT and IT security individuals in the U.S., the U.K., Germany and Japan and looks at the costs and benefits associated with such encryption. At that time, the costs of full disk encryption were estimated at $232 per user, per year. Using extrapolations, Ponemon estimates the cost savings from reduced data breach exposure to be $4,650. It should be noted that this study comes from an organisational rather than a manufacturer's perspective.

Some industry stakeholders suggested that the substantive costs of using alternative, secure and encrypted chips would add costs for industry, but these may not be as high as the concerns expressed by some stakeholders, if encrypted chips became industry standard due to EU regulatory requirements, which may be adopted in other jurisdictions internationally over time (based on previous experience under other EU legislation where other jurisdictions have introduced regulation subsequent to the EU being the first mover e.g. REACH, RoHS).

A further point raised by some interviewees from industry was that whilst some encryption technologies are more expensive, in other cases, encrypted components were found to have a similar cost as unencrypted, if carefully procured. It was therefore suggested that the costs of changing from a non-secure to a secure chip would result in only a marginal cost increase in components used in the manufacturing of internet-connected radio equipment. Other stakeholders expressed a different view as they said that encryption costs were high. This could be prohibitive in the case of low-priced products, where manufacturers' profits are slim.

The costs of security authentication: There may also be higher costs linked to the development of stronger authentication systems, and back-end product re-development. It was estimated by a gardening industry association that these could range around EUR 100,000, although this will depend heavily on the type of equipment. However, not all authentication implies significant costs, and there are potentially considerable benefits from strengthening security, given the importance of building and retaining trust among consumers. For example, two-factor authentication has now become common on many internet sites, and

[95] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). *Fog computing for the internet of things: Security and privacy issues.* IEEE Internet Computing, *21*(2), 34-42

[96] http://www.winmagic.com/ponemonstudy

extending this to internet-connected and/or wearable radio equipment need not be costly, as there are simple app's that can generate codes to authenticate the user, and many systems work based on sending an SMS to the user to verify their identity.

Overall findings: Overall, moving towards greater recourse to encryption and authentication would provide an effective technical solution to strengthening the security of internet-connected and/or wearable radio equipment.

There would be short-term costs of transitioning to ensuring that such products and devices are made more secure. The costs of chips and semi-conductors have been reduced over time, and if encrypted chips became the norm, then this could lower their cost. If the differential between encrypted and unencrypted chips could be made negligible, then this would create a win-win for the regulator, consumers, manufacturers and electronic components manufacturers.

As regards substantive costs, whilst some stakeholders, in particular industry associations, suggested that there would be high substantive costs of compliance incurred by manufacturers and other stakeholders in the value chain should this option be activated, others argued that these would be low. This is rather contradictory, in that some manufacturers already appear to be taking action to strengthen security in a way that protects users in terms of both data protection by design and default and protection from fraud. In addition, although recalling that "security by design" is already a legal obligation, it was not possible to assess in a quantitative manner the "differential" efforts that are needed to ensure compliance in case of adoption of this option. These differential costs can most likely be passed on considering the willingness to pay of consumers that have been estimated and reported in Table 3 below. It is also to be noted that the manufacturers' participation to the standardisation process is likely to mitigate further the risks of disproportionate costs.

Other categories of stakeholders (Consumers, MS, security industry) expressed the view that the substantive costs of compliance were likely to be low and highlighted that implementing baseline security requirements, such as changing default usernames and passwords and ensuring that other basic cybersecurity features are designed-in from the outset, would not be costly. These do not imply major product re-engineering (stakeholder from an MSA, several manufacturers interviewed for the product case studies). They added, however, that is important to be extremely clear in the definition of the technical specifications for baseline requirements, as uncertainties on this aspect may result in increased costs. Whilst implementing basic encryption to strengthen data protection and privacy was not seen as that costly, it was suggested that it could be prohibitive in terms of the costs per unit in some sectors. It was therefore stressed that the requirements can be a function of the equipment and the intended use.

There are high costs of data breaches and DDoS. These have been reported in Section 2.1. In instances when manufacturers of internet-connected and/or wearable radio equipment are already implementing security by design and default principles, it is expected that there are cost-savings for the equipment users associated with protecting different types of devices and products from security vulnerabilities through avoidance of the costs of data breaches. According to a study[97], manufacturers of cameras and routers who do not presently

[97] Irdeto Global Connected Industries Cybersecurity Survey (https://irdeto.com/news/new-2019-global-survey-iot-focused-cyberattacks-are-the-new-normal/)

implement adequate security by design and default, and/ or data protection by design and default account for circa 49% of the market. About half of the manufacturers would therefore incur new compliance costs under this option, whereas for the other half, the costs would be lower, reflecting the BaU costs (estimated at 70-80%), as some manufacturers are already following good practices in these areas. It is recalled that the costs of data breaches for companies were estimated at circa EUR 100.000 on average. It can therefore be argued that the high costs of a data breach means that it would be beneficial for the companies using the products to pay a higher price for more secure products.

Table 3: Estimated benefits from enhanced consumer trust and Willingness to Pay (WTP)[98] preferences

Product type	Impact on sales volume of products sold (%)	WTP for more secure products - % increase compared with baseline (%)
Routers	5%	10-15%
Laptops	5%	10-15%
Baby monitors	10%	10-15%
Security cameras	10%	10-15%
Smart domestic appliances	10%	5-10%
Robotic lawnmowers	5%	2%
Smart thermostats	5%	2%
All other internet-connected and/or wearable radio equipment, on average	5%	5-10%

Source: Commission's contractor[99]

Finally, under this option, the money lost due to financial fraud under the baseline will be mitigated, as well as identity thefts and the consequent resources that have to be spent to remediate possible matters (e.g. changing credentials, dealing with banks or credit card providers, etc). The extent will obviously depend on the applied technical solution.

In general, this policy option is opposed by the equipment manufacturers and was supported by the information security industry. Consumers' associations and several Member States also support its adoption, but would prefer to adopt Article 3(3)(d) jointly (i.e. option 5).

6.6. 6.6. Policy Option 5 – Article 3(3)(d), 3(3)(e) and 3(3)(f), focus on privacy and fraud protection and network security

The inclusion of Article 3(3)(d) ensures synergies with the objectives of protecting the networks. Specifically on 5G, that network will support the development of the Internet of Things and all 5G terminal equipment,

[98] concept relating to the maximum amount that consumers are willing to pay, in this case for internet-connected and/or wearable radio equipment with certain security features.
[99] https://ec.europa.eu/docsroom/documents/40763

including the mobile base stations, fall into the broader definition of "*internet-connected*[100] *and/or wearable radio equipment*".

The benefits described in the previous section would be strengthened through the adoption of a delegated act under Article 3(3)(d) together with those under Article 3(3)(e) and 3(3)(f). In particular, this option would allow a further mitigation of the DDoS risk, which can represent a significant cost for the society, including SMEs and other operators.

Also as regards reputational damage, users' trust in the Digital Single Market, improved functioning of the Internal Market and competitiveness of EU industry, the same considerations of the previous sections apply, magnified by the increased protection that this option will entail. The interview programme with manufacturers also found that certain leading European manufacturers in some product groups for internet-connected and/or wearable radio equipment are investing significant resources in strengthening product security to enhance their brand's reputation, by building security into their value proposition. The feedback was that some of the leading European manufacturers believe they could potentially strengthen Europe's industrial competitiveness by investing further in product security, as Europe has a strong reputation in the field of security, which could help to differentiate it from competitors globally and boost the development of technological sovereignty. Whilst the considerations in this paragraph generally apply to all the policy options so far discussed, it is reported under this policy option as the more security is demanded under the options, the bigger the impact is likely to be.

As regards SMEs, approximately 25 million SMEs were estimated to operate in the EU in 2018[101] and 2019[102], in the non-financial sector. Approximately 87.000 companies were estimated to be manufacturers in the EU 27 with NACE[103] codes 26 (35.000) and/or 27 (42.000)[104], i.e. manufacturers of computer, electronic and optical products and manufacturers of electrical equipment, which include manufacturers of internet-connected and/or wearable radio equipment. Out of these, only 4.500 are reported to be manufacturers of communication equipment (NACE code 263), although more and more manufacturers of conventional goods are making their products connectable. In addition not all these manufacturers are SMEs. As a consequence, the number of European SMEs which will have to comply with this new initiative accounts for between 0.018% and 0.35% of the total. Finally, a relevant consideration is that the EU SMEs are typically either assemblers of components or software developers on existing hardware. Most of the components and hardware comes from outside the EU, hence the value chain considerations (see section 6.5) will minimise the efforts required by the SMEs to demonstrate conformity to the RED.

In the Expert Group of Radio Equipment[105], an association of SMEs confirmed their support to this initiative subject to avoidance of lock-down of equipment. The Commission services are already aware of this matter, which concerns more Article 3(3)(i) than 3(3)(d/e/f), as confirmed by recital 19 of the RED, and will address any possible related issue in the parallel initiative concerning the upload of software.

---

[100] as defined in section 2, i.e. capable itself to communicate over the internet, regardless if it communicates directly or "indirectly", i.e. via any other equipment.

[101] https://ec.europa.eu/growth/smes/business-friendly-environment/performance-review_en

[102] https://epthinktank.eu/figure19e28093keyfiguresonsmesintheeuropeanunion

[103] Nomenclature statistique des Activités économiques dans la Communauté Européenne

[104] https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=sbs_na_ind_r2&lang=en

[105] https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/95449c1e-11be-4233-b93c-da29de18780f?p=1&n=10&sort=modified_DESC

As regards costs for manufacturers of equipment, being them large companies or SMEs, the quantitative analysis for Article 3(3)(e) and 3(3)(f) is the same as for option 4, noting that the ESOs have started the production of reports and technical specifications for complex systems. These include protection of the networks together with privacy and fraud matters. There are already products that can benefit from the flourishing production of standards and technical specifications in this field. An example that can allow clarifying the commonalities across Articles 3(3)(d), (e) and 3(3)(f) is EN 62 443-4-2:2019 concerning "*Security for industrial automation and control systems; technical security requirements for IACS*[106] *components*", which was suggested by CENELEC as one of the standards that may be used as a basis for future possible harmonised standards. Out of 56[107] technical clauses of that standard that are assumed to relate to Articles 3(3)(d), 3(3)(e) and 3(3)(f)[108]:

- 52 (93%) concern Article 3(3)(e);
- 52 (93%) concern Article 3(3)(f);
- 51 (91%) concern both Articles 3(3)(e) and 3(3)(f);
- 44 (79%) concern Article 3(3)(d);
- 40 (71%) Articles 3(3)(d) and 3(3)(e); and
- 39 (70%) concern Articles 3(3)(d), 3(3)(e) and 3(3)(f).

This means that for this specific equipment, it can be estimated at this stage that 98% (51/52) of the clauses that can be used to cover the risks under Article 3(3)(e) can be used to cover the risks under Article 3(3)(f) and 91% (40/44) to cover the risks under Article 3(3)(d). If both Articles 3(3)(e) and 3(3)(f) are implemented, 89% (39/44) of the used technical solutions can be also used for Article 3(3)(d). Even if these percentages are estimates based on one standard only, they allow noting that:

- A very high percentage of the technical solutions addressing Article 3(3)(e) can be used as well for addressing Article 3(3)(d) and/or 3(3)(f). The GDPR is already applicable so this reinforces that most of the costs have (or should have) already been incurred;
- There is a degree of coherence in adopting a delegated act pursuant Article 3(3)(d) as a complement to those under Article 3(3)(e) and 3(3)(f). This will ensure that the inherent synergies between these three Articles will be used at the best, mitigating the costs for the society and the stakeholders;
- There are yet some differences between Articles 3(3)(d), 3(3)(e) and 3(3)(f), meaning that some risks may remain if not all three are invoked. Because of the commonalities in the technical

[106] Industrial Automation and Control Systems
[107] There would be even more clauses, but a clustering of clauses with same requirements for different use-cases has been performed. The figures that follow have to be taken consequently as a conservative estimate.
[108] For completeness, the analysis also considered Article 3(3)(i). For this Article, 36 clauses are presumed to relate Article 3(3)(i) and 32 to all Articles 3(3)(d), 3(3)(e) and 3(3)(f).

solutions, the adoption of the 3 delegated acts will imply costs that can be comparable to the adoption of one act only.

The Commission services will follow-up this initial analysis, also with the help of the Expert Group on Radio Equipment, in view of a possible future standardization request.

In conclusion, (i) as regards frauds for non-cash payments, there are approximately EUR 1.8 billion of costs that citizens can potentially save, whilst other costs are not quantifiable, see section 2.1.2, (ii) the cost of data breaches are at least EUR 10 billion, see section 2.1.3 and (iii) the costs of DDoS are estimated to be at least EUR 65 billion, see section 2.1.3. It is clear that not all costs above can be avoided by this initiative, but it aims to mitigate the risks of their occurrence when radio equipment is used. Prospective business opportunities in a secure digital single market (DSM) account for approximately EUR 36 billion over the next 10 years (3.6 billion a year on average), only for 5G-related technologies, see section 2.3. The precondition is to have a secure DSM. This initiative will contribute to it, proportionally to the covered equipment and the risks. As already discussed in section 2.4, the COVID crisis is expected to further increase the costs to society presented in this paragraph.

The possible benefits and reduction of costs herein described do not take into account the following, which are hard to quantify, but can be very significant: (i) the non-quantifiable increase in consumer trust, (ii) the costs that should have been already sustained under the GDPR, (iii) the savings for network operators in case of an increased protection of the networks, (iv) the costs of reputational damage and (v) the increase of revenues due to the expected willingness to pay for safer products, (vi) possible impacts of non-action on the Internal market and (vii) possible impacts of non-action on the competitiveness. It is important also to flag that the provided costs, e.g. in table 2, concern each single model of radio equipment in scope. Unfortunately, whilst the volumes are expected to increase as in table 1, no information was provided by the associations or by individual manufacturers on the expected numbers of models, and their trends, which will be placed on the EU market. As a consequence, the full costs for the manufacturing sector could only be estimated per each single model which would be placed on the EU market, not in aggregate. As regards MSA, in 2018 16 EU Countries, representing approximately 70% of the EU population, verified the compliance of 3341 models of equipment[109]. Assuming that the same number of models will be assessed in the future and assuming that also the other MS, representing approximately 30% of the EU population, assessed a proportional number of models, it can be assumed that approximately 5000 models have been assessed. At an average cost of 7500 EUR per model, the costs for enforcing these new requirements are estimated in less than 40 million EUR.

This policy option was strongly supported by MS in the Expert Group on Radio Equipment and consumers associations[110]. It also found the support of stakeholders representing security firms in the Expert Group of Radio Equipment and, conditionally, at least one association of SMEs. In general terms, it is opposed by equipment manufacturers.

[109] https://ec.europa.eu/docsroom/documents/36941

[110] see documents in the relevant repositories of the TCAM WG https://circabc.europa.eu/ui/group/bf6f7fb7-502b-431c-9ae0-36d206b48817 and EG RE https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe

7. 7. HOW DO THE OPTIONS COMPARE?

Table 5 provides information comparing the policy options in terms of effectiveness (how each option achieves the specific objectives) and efficiency (cost-benefits analysis) and coherence with other pieces of EU law. Table 6 compares the impacts of the policy options on stakeholders.

Table 5: comparison of policy options

	Effectiveness	Efficiency	Coherence
Policy option 0	This policy option will not ensure protection of the equipment, unless this is done by individual manufacturers on a voluntary basis.	This policy option will not introduce costs on manufacturers of equipment, but all other costs described in section 2.1 will be borne by the users and society. Competiveness, functioning of the internal market and consumers' trust will not be ensured.	Under this option, there will be no mandatory requirements for manufacturing in support of the policy objectives of the legislation in Annex 6 and no enforcement will be possible.
Policy option 1	This policy option will not ensure protection of the equipment, especially in the absence of ongoing voluntary initiatives.	This policy option will not introduce major costs on manufacturers of equipment, but all other costs described in section 6.2 will be borne by the users and society. Competiveness, functioning of the internal market and consumers' trust will not be ensured.	Under this option, there will be no mandatory requirements for manufacturing in support of the policy objectives of the legislation in Annex 6 and no enforcement will be possible.
Policy option 2	This policy option will ensure protection of privacy only. As such, certain specific objectives (e.g. protection of the networks, protection from fraud) could not be attained.	This policy option will introduce costs on manufacturers of equipment, and a mitigation of the other costs, as described in Section 6.3. Most of the costs of manufacturers should have been incurred already in 2018 with the applicability of the GDPR. Competiveness, functioning of the internal market and consumers' trust will be ensured in part.	This option will support the policy objectives in the GDPR and the ePD, allowing to place equipment on the market only if the "security by design" and the support to confidentiality of communications is demonstrated. Neither protection from fraud nor protection of the networks will be ensured.
Policy option 3	This policy option will ensure protection from fraud only. As such, certain specific objectives (e.g. protection of the networks, protection of privacy) could not be attained.	This policy option will introduce costs on manufacturers of equipment, and a mitigation of the other costs, as described in Section 6.4. Competiveness, functioning of the internal market and consumers' trust will be ensured in part.	This option will support the policy objectives in the of non-cash payment Directive. It will not allow to enforce the "security by design" principle in the GDPR and the support to confidentiality of communications in the ePD. Protection of the networks will not be ensured on the equipment side, as a condition

			for market access.
Policy option 4	This policy option will ensure protection of privacy and from fraud. As such, the specific objective regarding protection of the networks could not be attained.	This policy option will introduce costs on manufacturers of equipment, and a mitigation of the other costs, as described in Section 6.4. Competiveness, functioning of the internal market and consumers' trust will be ensured in part.	This option will support the policy objectives in the non-cash payment Directive, the GDPR and the ePD. Protection of the networks will not be ensured on the equipment side, as a condition for market access.
Policy option 5	This policy option will ensure the highest level of protection, given the empowerment in the RED and allow achieving all specific objectives.	This policy option will introduce costs on manufacturers of equipment. The great part of these costs have already been incurred to comply with the GDPR and Articles 3(3)(d), 3(3)(e) and 3(3)(f) appear to be addressable to a good extent through the same technical solutions. Their possible extra costs will be further mitigated through harmonised standards, whilst the majority of the citizens and the network operators will have significant advantages, as described in Section 6.5.	This option will support the policy objectives in all the legislation in Annex 6. With respect to policy Option 4, the protection of the networks can also be ensured as a condition for market access.

Table 6 shows to which extent the specific policy objectives in section 4.2 are fulfilled by the different policy options.

Table 6: policy objectives and policy options

Options	Respect of fundamental rights	Timely action	Trust in DSM and new technologies	Allowing enforcement	Preservation of the Internal market	Level-playing field
Policy option 0	*no change*	*No*	*no change*	*No*	*No*	*no change*
Policy option 1	*P*	*P*	*P*	*No*	*No*	*P*
Policy option 2	+	+	+	+	+	+
Policy option 3	+	+	+	+	+	+
Policy option 4	++	++	++	++	++	++
Policy option 5	+++	+++	+++	+++	+++	+++

Legend: P Proportional to the number of volunteers; + reduced positive impact; ++ positive impact; +++ significant positive impact

The assessment of the impacts can be visualised as follow:

Table 7: Impacts of policy options

Options / impacts, relative to the baseline	Economic impacts	Social impacts	Environmental impacts[111]
Policy option 0[112]	*no change*	*no change*	*no change*
Policy option 1[113]	N/A	N/A	*no change*
Policy option 2[114]	+	+	*no change*
Policy option 3[115]	+	+	*no change*
Policy option 4[116]	++	++	*no change*
Policy option 5[117]	+++	+++	*no change*

Legend: N/A not applicable; + reduced positive impact; ++ positive impact; +++ significant positive impact

The overall position of the Member States and stakeholders can be visualised as in the following table:

Table 8: position of Member States and stakeholders

Options	Member States	Consumers Associations	Equipment manufacturers	Information security industry
Policy option 0	---	---	+++	-
Policy option 1	---	---	+++	-
Policy option 2	+	+	--	+
Policy option 3	+	+	--	+
Policy option 4	++	++	--	++
Policy option 5	+++	+++	---	+++

Legend: - not so in favour; -- not in favour; --- completely adverse; + marginally in favour; ++ in favour; +++ significantly in favour

Finally, the overall comparison between attainment of objectives and the increase of costs for equipment manufacturers (see section 6.6) can be visualised as in the following table:

[111] The general considerations in section 6 apply, but they are not sufficient to assume a positive impact of policy options 2, 3, 4 or 5
[112] See section 6.1
[113] See section 6.2
[114] See section 6.3
[115] See section 6.4
[116] See section 6.5
[117] See section 6.6

Table 9: policy objectives and costs for equipment manufacturers

Options	Attainment of benefits/policy objectives	Increase of costs (assuming not already taking into account security by design in the GDPR)	Increase of costs (assuming taking into account the security by design in the GDPR)
Policy option 0	*no change*	*no change*	*no change*
Policy option 1	*Proportional to the number of volunteers*	*Proportional to the number of volunteers*	*Proportional to the number of volunteers*
Policy option 2	+	+	*no change*
Policy option 3	+	+	+
Policy option 4	++	++	+
Policy option 5	++++	+++	++

Legend: + marginal increase; ++ moderate increase; +++ significant increase; ++++ very significant increase

This last table shows that the highest benefits can be achieved with an initiative which is as broad as possible. At the same time, the costs for the equipment manufacturers who already comply with the applicable EU law will be moderate.

8. 8. PREFERRED OPTION

8.1. 8.1. Preferred policy option: option 5

In light of the data and the considerations in the previous sections, the preferred policy option is option 5. This would strengthen the RED's essential requirements to close regulatory loopholes as much as possible, in a coherent and timely manner. All internet-connected[118] and/or wearable radio equipment will be in the scope of such act. Specific attention shall also be paid to the privacy issues in toys and equipment for childcare, being children a category of most vulnerable users. In line with the risk-based approach, the applicability of the three articles will be modulated on the basis of the equipment's capabilities.

As regards the further proportionality of the selected policy option, following the adoption of the delegated act(s), the European Commission will issue a standardisation mandate to the ESOs. This would allow the stakeholders, in particular the industrial sector, to lay down different technical solutions as a function of products and risks. In turn this will avoid to mandate disproportionate solutions. There are already existing solutions which can be used. For privacy, the "security by design" principle of the GDPR can already be addressed through specific standards. The same applies to the security of payments. For the protection of the network, there is already a pool of best practices and standards that stem from the implementation of the NIS Directive which can be taken as a benchmark and mirrored, where appropriate, into the design of equipment. In the specific case of the CSA, the presence of voluntary certification schemes will help the standardisation of the RED, as these schemes will represent a benchmark for the expected level of protection that the

[118] as defined in section 2, i.e. capable itself to communicate over the internet, regardless if it communicates directly or "indirectly", i.e. via any other equipment.

equipment has to demonstrate for the purposes of market access. In such cases, the ESOs would be then expected to reflect into harmonised standards the relevant parts, which concern manufacturing and verify at the same time that their content meets the minimum needed quality to allow manufacturers to presume conformity of the equipment with the RED essential requirements. This will ensure that the implementation of these pieces of EU legislation creates synergies avoiding conflicting technical specifications. The Commission services have established a strong cooperation to monitor those specific developments and to keep a coordinated approach.

It is then clear that the availability of all these standards (or schemes) and the industrial involvement in the standardisation exercise limits already the risks of imposing a disproportionate burden to demonstrate compliance with the RED. The ESOs are already working closely with industry, all relevant Authorities of the Member States and the Commission Services to anticipate the needed steps to timely deliver harmonised standards.

It is also worth mentioning explicitly that these harmonised standards will be performance-based and technology neutral. This will limit the risk of hindering innovation. The specific exclusion in Annex I of the RED for specific research equipment, as described in section 1, will further limit this risk.

With specific respect to the impact on SMEs, as noted in section 6.6, only a minority of EU SMEs may be affected and in any case the presence of standards will reduce costs especially for them. The broad scope of the initiative, where also components are included, will also guarantee that the new requirements can be demonstrated throughout the value chain, limiting the costs on the manufacturer (including SMEs) at its end.

As regards competitiveness, this option will improve the level playing field between manufacturers who have already sustained costs to comply with the applicable related legislation and those manufacturers who, in the absence of effective enforcement tools, paid little attention to design secure equipment.

In the absence of an EU law, certain national schemes based on third party certifications are emerging. Whilst they are generally voluntary, and possibly for specific niche sectors they are mandatory. Different schemes can have different technical requirements and they are subject to the type approval regime. Once/if they become mandatory, they can be therefore more costly than the RED regime where, if harmonised standards are used, self-certification applies.

Finally, it is worth noting that this option will not address products which are already on the market or will be placed on the market before the date of applicability of the delegated act. In general, on the one hand, for matters of predictability and legal certainty, there is a delay between the entry into force of an act and its applicability. On the other hand, certain internet-connected radio equipment and/or wearable radio equipment have a short life-cycle, and are sold in volumes, so the uptake of security measures under this option can produce its effects on a large scale relatively quickly after the date of applicability.

8.2. 8.2. REFIT (simplification and improved efficiency)

REFIT considerations are not applicable, as this initiative is not a revision of Directive 2014/53/EU, but a delegated act pursuant to its Article 3(3).

The preferred option will not change any other applicable provision of the Directive, with the exception of bringing the categories of equipment described in the first paragraph of the previous section (8.1) in scope of Articles 3(3)(d), 3(3)(e) and 3(3)(f).

9. 9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

After the entry into force of the preferred option, the Commission will monitor the implementation, the application and the compliance to these new provisions with a view to assessing their effectiveness. The Commission is under the obligation to monitor and report the implementation of the Directive to the Council and the European Parliament. A review is due by 12 June 2023. As manufacturers will be given sufficient time to adapt to the new essential requirements and demonstrate the needed compliance, through a delayed date of applicability, in 2023 implementation aspects will be examined. The report of 2028, or earlier evaluations of the Directive, will deliver a more complete review, including administrative and compliance costs. The monitoring framework would also account for the information reported under the related pieces of EU law in Annex 6. This collective source of information will create an evidence base for a future assessment of the functioning of the intervention.

Operational objectives are (1) to ensure adequate implementation of the new rules supported by harmonised standards and timely assessment of new products by Notified Bodies, (2) to ensure adequate application of the new rules in practice and to identify any remaining gaps, and (3) to ensure enforcement of the rules by national authorities.

- On the implementation, the Commission will spend significant efforts to ensure that the conformity assessment of radio equipment can be performed smoothly. This means that a standardization request will be issued and its implementation will be followed. As discussed, preliminary work has already started. In parallel, the Commission will verify that the capacity of Notified Bodies is not reached. In accordance with Article 47(2) of the Directive, the Commission will report the state-of-play of the implementation of the Directive, including the aspects herein discussed, to the Council and European Parliament by 2023.
- On the application, by means of the reports of Member States in Article 47(1), the Commission will verify that national initiatives do not concern aspects covered by the Directive, including the new provisions herein discussed.
- Whereas the main added value of this initiative under the RED is to allow that the policy objectives of other applicable legislation in Annex 6 can be enforced as a condition of market access, the general effectiveness on security matters will be monitored in conjunction with the relevant pieces of EU law, and the Commission will monitor the reports of Market Surveillance Authorities, which are regularly submitted to the Expert Group on Radio Equipment.

In more detail these can be described as follows:

Table 10: monitoring strategy

Stage	Indicator	Definition	Unit of measurement	Data source
Implementation	Harmonised standards	As in the Standardisation Regulation 1025/2012	Number of produced harmonised standards / approximate market share of covered equipment	ESOs, internal Commission databases, Eurostat
Implementation	Capacity of Notified Bodies	Average number of days to assess a product	Number, as compared to the current situation	Notified Bodies

Application	National initiatives	Initiatives at national level that aim to address possible related problems or gaps which could not/were not addressed through this initiative	Number of MS where these initiatives are running	Member States, Article 47(1)
Application	Possible remaining gaps/problems		Severity of potential remaining problems	Member States and stakeholders in general
Application	Evaluations, revisions and reports under the related EU law	Initiatives at the EU level that aim to address possible related problems	Evolution of the problems that drove the establishment of the related frameworks in Annex 6	Member States and stakeholders in general
Enforcement	Statistics of Market Surveillance or other EU Authorities	Reports	Percentage of non-compliant equipment	Member States

ANNEX 1: PROCEDURAL INFORMATION

10. 1. LEAD DG, DECIDE PLANNING/CWP REFERENCES

The lead DG is the DG for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW). The Directorate in charge was Directorate C - Sustainable Industry and Mobility. The internal Planning entry was PLAN/2018/3135.

11. 2. ORGANISATION AND TIMING

An Interservice Group was set up with the participation of DG GROW, DG CNECT, DG COMP, DG DEFIS, DG JRC, DG JUST, DG HOME, DG MOVE, DG L, DG SANTE, DG SG, DG TRADE.

Meetings took place on 6th September 2018, 18th October 2019, 9th December 2019 and the final meeting on 4th September 2020.

12. 3. CONSULTATION OF THE RSB

This impact assessment was discussed at a meeting with the RSB on 14th October 2020.The RSB issued its opinion on 16th October, following which this impact assessment has been revised as follows:

In general, Sections 1, 2, 4, 5.2, 5.3, 6.5, 8.1 underwent major revisions. A new Annex 7 was added. Moderate changes were introduced in Sections 6.6, 7, 9 and Annex 8 (Annex 7 of this final document). Minor revisions concerned the rest of the text. Details on the comments and changes are reported below

Summary of findings	
1. The context of the proposal and its scope are unclear. The report does not sufficiently explain how this initiative fits with other related initiatives.	(i) Section 1 has been significantly revised, improving the relationship with the other initiatives and EU legislation; (ii) Section 1 also clarifies better which equipment is in scope or out of scope of the Directive in a more explicit manner; (iii) Section 2 includes now a further clarification on equipment which is not in scope of the initiative, e.g. non-internet connected radio equipment and equipment connected to the internet only by cables;
2. The report is not sufficiently precise on the problems that the initiative would solve.	(i) Section 1 has now a clear reference to "mandatory market access conditions" and "corrective measures on non-compliant equipment"; (ii) Section 2, on the problem definition and drivers, has been significantly revised, describing in a more accurate manner the reasons for this initiative; (iii) A problem tree was inserted in Annex 7;
3. The report does not clearly justify the range of options it retains for the analysis, and why it discards other plausible options.	(i) Additional explanations were inserted in Section 5, with specific respect to section 5.2; (ii) Section 5.3 now reports the disregarded options in bullets, with an improved explanation;
4. The report is not sufficiently clear about the proportionality of the preferred option and what role the subsequent standardisation process will play.	(i) Section 8.1 was completely revised to take into account this comment.

What to improve	
1. The report should better explain the context of this initiative. It should clarify the cybersecurity policy landscape, which issues are being tackled by existing measures, within which timeframe and where there are gaps or issues that would warrant further action. The report should then explain the role of radio equipment within the wider cyber-security context.	(i) Most of the needed changes on the cybersecurity landscape are now reflected in the revised Section 1; (ii) Gaps and issues are now described in a better manner in Section 2 and summarised in Annex 3; (iii) The timeframe of the applicability of a regulatory initiative is now explained in Section 1. The timeliness of EU action has been highlighted in sections 3.2 and 4.1, and in parts of Section 5; (iv) The role of radio equipment in the cybersecurity context has been strengthened in Section 1 and at the end of section 2.1.3;
2. The report should clarify the scope of this initiative. It should specify which equipment is covered. It should clarify whether it would only concern new products placed on the market or be retroactive.	(i) The revised Section 2 now clarifies explicitly which equipment is in scope of the initiative and which is not. It complements the information in Section 1 on the equipment that is in scope of the Directive; (ii) Section 6.5 clarifies the need to have equipment in the value chain in scope of the initiative; (iii) As regards the issue of retro-applicability of the preferred option, this is explained at the end of Section 8.1, also with a qualitative analysis on the effects of the date of applicability on the impacts of the initiative;
3. The report should be clearer on precisely what problems this initiative will fix. It should be more specific on the role of lacking security of radio equipment in these problems. It should clarify the role of equipment security in overall network security.	(i) In order to enhance the understanding of which problems will be fixed and how, a problem tree was introduced in Annex 7; (ii) The lack of security in radio equipment has been demonstrated through links to appropriate reports (see footnotes 8, 9, 16, 17, 19) and has been reinforced throughout Section 2 and 2.2. Section 4.1 clarifies that the selected scope ("internet connected and/or wearable radio equipment") is the one presenting most risks; (iii) The relationship between radio equipment and network security has been explained in Section 1. Further minor clarifications have been added in sections 2.1.3, 6.6 and 8.1 for the relevant aspects.
4. The report should make clear that other initiatives will deal with aspects of the identified cybersecurity problems. It should explain possible timing differences between initiatives and discuss their coherence (or lack thereof).	(i) Other initiatives related to cybersecurity have been taken into account in the general introduction in Section 1, to be read in conjunction with Annex 6; (ii) As regards a possible future horizontal mandatory framework, which would require co-decision, Section 5.3 clarifies why it was not considered in the first place;
5. The intervention logic should be adapted to a revised policy context and problem description. It should focus directly on the problems that this initiative will target. The specific objectives could include enforceability and timing, which are important features for the initiative.	(i) Section 1 clarifies now how a delegated act under the RED can ensure timeliness, relying on empowerments already granted by the co-legislators which do not require a full co-decision process; (ii) Section 4 has been redrafted following the revised policy context and problem description; (iii) Annex 7 has been inserted in support of a thorough understanding of the intervention

	logic; (iv) As a complement, some text was added in Section 2.4 following a recent report; (v) Enforceability and timing were included in the objectives and supported by explanations in the rest of the text (mostly Sections 1 and 2);
6. The current options design is limited to possibilities for action available through the radio equipment Directive. The report should discuss why potential alternatives, reflecting different implementation modes (i.e. a labelling/certification scheme) or a solution at the network level have been rejected as not credible. Moreover, the report should better substantiate discarding the option of a horizontal cybersecurity legislation upfront.	(i) Section 1, to be read in conjunction with Annex 6, now makes clear the legal interactions and scopes of the existing legislations, including solutions at the network level; (ii) As regards a possible future horizontal mandatory framework, which would require co-decision, Section 5.3 clarifies why it was not considered at this stage. The same section also explains why a stand-alone option of Article 3(3)(d) was not considered; (iii) Additional clarifications were added in section 8.1, explaining in more detail how implementing measures of the RED and the CSA/NIS can coexist and be coherent with one another;
7. The report should better justify the proportionality of the preferred option. It should clarify that technical solutions will be developed with stakeholders, including industry, in the European Standards Organisation context. The report should describe how this will ensure proportionate outcomes and how technical solutions will differentiate according to products, based on the nature of risks involved. The report should also demonstrate that the approach taken will not be disproportionate relative to possible technical solutions at network level. It should also assess if SMEs might be disproportionately affected and, if so, how this could be mitigated. The report should analyse what impact the preferred option would have on innovation. It should also acknowledge that even with the preferred option, some risks will remain (including for products already sold on the market).	(i) The suggested improvements led to a thorough revision of Section 8.1, which includes thorough considerations on proportionality. It includes specific consideration on the value chain and an exemplification of the current practice to reuse parts of conformity assessment procedures from suppliers; (ii) The same section also exemplifies that the ESOs will be called to produce technical specifications to proportionally cover risks and how these technical specifications are expected to be technology neutral and performance based, not to prescribe specific technologies which could limit innovation; (iii) As regards innovation, the point above has also to be read in conjunction with section 1, where a reference to the clear exclusion in the basic act for certain R&D products has been inserted. In the same Section, it is explained that a transition period will be given as regards the introduction of the new requirements and to which extent the date of applicability of the act is a trade-off between the need of secure products, the economic interests and the expected life-cycle of the equipment; (iv) As regards SMEs, sections 6.5 and 6.6 now contain a more specific description of the cost-benefit analysis for SMEs and how they can benefit from a scope that distributes the demonstration of compliance proportionally through the value chain; (v) Finally, Sections 1, 2 and Annex 3 clarifies that there will still be risks for wired-only connected products, but that, on a statistical basis, however, it is likely that most of the incidents occur by means of radio equipment, as more and more products have a wireless functionality. As regards the remaining risks given a date of applicability in the future, considerations have

	been reported in section 1 and at the end of section 8.1.

Following the modifications above, the RSB was consulted on 21st December 2020. The RSB issued its positive opinion on 22nd January 2021, recommending to further improve the analysis as below:

Summary of findings	
1. The report does not contain a complete intervention logic. It does not include the timing and enforceability aspects and does not build on specific objectives.	(i) The former Annex 7 with the intervention logic has been incorporated as figure 2 in the text; (ii) The specific objectives have been modified to include timing and enforceability;
2. The report does not sufficiently assess enforcement costs. The summary table of costs and benefits is not precise or sufficiently comprehensive.	(i) The number of models placed on the EU market each year were not available. Lacking these data, certain costs could be reported only per model, not in aggregate. For enforcement, these numbers were estimated base on a 2018 report of activities.

What to improve	
1. The report should revise the intervention logic and include it in the main body of the report. The intervention logic should account for timing and enforceability concerns that are important for the decision at stake. While these elements are mentioned in the text, they are not integrated in the analysis in a structured way. The intervention logic should include a set of clear and specific objectives, which should be used in the assessment and comparison of options.	(i) Timeliness and enforceability was inserted in the specific objectives so to achieve coherency with the text in section 5.3; (ii) The former Annex 7 with the intervention logic has been revised and incorporated as figure 2 in the main text; (iii) Section 7 has been improved by including a new table showing the extent to which each options allows achieving each of the specific objectives.
2. The report should provide a clearer explanation why any policy option addressing only the network level (rather than the specific connected equipment as such) would be insufficient for ensuring security.	(i) Text was added at the end of section 5.3; (ii) For clarity, a sentence in section 2.1.3 was added to reinforce that the actions pursuant this initiative would be complementary to other actions at the network level.
3. The summary table in annex of the report should include a clearer indication of the proportion of the estimated direct benefits that would stem from this initiative. It should also add enforcement costs and take over the estimates of the total annual (one-off and recurrent) administrative costs for businesses, based on the estimates for testing costs per equipment mentioned in the main report.	(i) It was explicitly added to section 6.6 and Annex 3 that the absence of specific data concerning the volumes of models placed on the EU market makes it impossible to estimate the aggregate costs for the manufacturing sector. For MSA an estimate was inserted.

13. 4. EVIDENCE, SOURCES AND QUALITY

A study[119] supporting this impact assessment has been carried out by consultants The Commission's consultants carried out a number of interviews, analysed the data from the public and the targeted consultations, complementing them through desk research and other case studies.

[119] https://ec.europa.eu/docsroom/documents/40763

Evidence was also gathered in the Expert Group on Radio Equipment, interview with stakeholders and through public or targeted consultations.

Whenever quantitative information has been sought, EU sources were preferred (e.g. reports or statements from ECB, EU Court of Auditors, Eurostat, EU Agencies, other EU Bodies, etc). Other sources were also considered (e.g. studies or reports of international organisations or firms, of associations of stakeholders, etc). The sources have been chosen, consequently, as reliable as possible. Similar data, when possible, were cross-checked. It is acknowledged that some data are estimates. In order to compensate for possible inaccuracies, throughout this document benefits were repeatedly estimated in a conservative manner.

ANNEX 2: STAKEHOLDER CONSULTATION

Radio equipment and radio technologies are a key enabling part of the ongoing and forthcoming deployment of new technological developments and/or environments, for this reason the consultation strategy 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, in particular those relating to (cyber)security, data protection and privacy.

In this framework, the consultations aimed (i) to provide the Commission with a thorough and comprehensive outlook of the regulatory initiatives that may be undertaken in order to implement the Digital Single and Internal Market, in line with its priorities and (ii) at capturing the views of all relevant stakeholders, allowing them to provide their feedback on these main issues and possible solutions. Feedback provided by stakeholders were used for the scope of this analysis 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 (manufacturers, distributors, importers), including SMEs, operating in the field of radio equipment;
- Individual of economic operators (manufacturers, distributors, importers), including SMEs, operating in the field of radio equipment;
- Associations of economic operators, operating in the field of digital security;
- Individual economic operators, operating in the field of digital security;
- Consumer organisations
- Citizens
- Academic/research institutions and relevant non-governmental organisations
- Notified bodies
- Standardisation Organisations

The following specific consultation activities has been carried out:

- All interested stakeholders could provide feedback on the inception impact assessment over a four week period[120];
- A 12-week public consultation has been launched on the Commission's Better Regulation Portal[121];
- A targeted consultation addressed specifically Member States, economic operators (associations or individual), consumer organizations, compliance assessment bodies, consumers or other experts.

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

Structured/semi-structured interviews complemented the targeted consultations. Details are in the table below. A workshop was also organised on 25th June 2019 in the Expert Group on Radio Equipment E03587.

A detailed summary of these consultations can be found in the report of the Commission's contractor[122].

Interviews

Table 11: interviewed stakeholders

Organisation type	Interviewed
Academia	5
European bodies	3
European Industry Association	14
European Consumer Associations	5
ESOs	2
International consumer association	1
International industry association	1
Manufacturers (of which SMEs)	25 (8)
Market research	1
National Authorities (of which data protection Authorities)	12 (2)
Notified body	1
Testing & certification bodies	6
Other private sector (consulting firms, insurance companies, cybersecurity firms)	5
Total	**76**

The stakeholder consultations found there to be a broad consensus among stakeholders that different categories of internet-connected and/or wearable radio equipment have at least some security vulnerabilities, some common to the device being directly connected to the internet across all product groups. Other vulnerabilities of device penetration are associated with particular categories of such radio equipment.

There was also agreement that wired products directly connected to the internet often have similar vulnerabilities. However, these are outside the RED's scope, which led some stakeholders, especially from industry associations and individual manufacturers to question whether it was coherent to legislate differently between wireless and wired products.

Many stakeholders interviewed acknowledged that it is difficult to determine the relative number of vulnerabilities and the corresponding level of risk associated with different connected radio products, as the nature of security vulnerabilities and threats, especially in relation to fraud, evolve rapidly.

Stakeholders recognised that if a regulatory option is to be activated, it would be quite difficult to make the essential requirements only applicable to directly internet-connected radio equipment using a RLAN connection, as Bluetooth and other similar communications protocols allow for wireless data sharing and are connected to the internet, albeit indirectly. Although simple short range devices are arguably at lower risk of

[122] https://ec.europa.eu/docsroom/documents/40763

being penetrated since a user would need to be in close proximity, it would be difficult to regulate only RLAN products, but not products with other radio capabilities.

Stakeholders had divergent views as to how best to address the identified security vulnerabilities that could compromise personal data protection and privacy in terms of technical solutions that could address the risk of device penetration, and as to whether a regulatory approach was necessary or not.

Consumer associations, national authorities and market surveillance authorities were generally in favour of taking regulatory action to address vulnerabilities, whereas about half of industry associations and many manufacturers and other economic operators had concerns about a regulatory approach as to the risk of duplication with existing regulatory requirements under the GDPR and e-PD.

Some stakeholders, especially industry associations noted that there has been insufficient time to gather an evidence base as to the effectiveness and efficiency of recently introduced EU legislation as the GDPR came into effect in May 2018 and the CSA on 27th June 2019. Moreover, no (voluntary) certification schemes have yet been implemented through the CSA as these are still under discussion (coordinated by ENISA).

Whilst there were disagreements depending on the type of stakeholders as to the best policy means of addressing the problem of identified security vulnerabilities in internet-connected radio equipment, it was widely recognised that trust in such products and devices, especially in consumer IoT, where many of the problems are more acute due to the products being cheaper, could be undermined unless actions are taken to improve the current situation in respect of the presence of unsecure products on the European market.

Stakeholders taking part in the targeted consultations made clear that even with a regulatory approach supported by harmonised technical standards, it could not be guaranteed that internet-connected and/or wearable radio equipment are secure, as new security vulnerabilities are frequently identified, and are already designed out as part of the development of next-generation technologies, products and devices. Therefore, minimum baseline requirements, whilst a positive step in the views of many stakeholders (including the great majority of national authorities and MSAs) would need to be kept under review, and standards updated accordingly.

Targeted consultation

Stakeholders were 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. It should be noted that the selected stakeholders were free to respond or not respond, so the sample has a degree of self-selection and is not necessarily representative of the overall cohort of stakeholders. A number of responses across multiple respondents contained significant repetition, suggesting a co-ordinated response.

The online questionnaire consisted of both open and closed questions. The statistics stemming from the closed questions are presented in the contractor's study. The answers to the open questions have been analysed thoroughly and used to complement a number of quantitative answers. However, since the open questions were optional and only a minority of respondents answered them, the responses to open questions have been used exclusively in a qualitative way (with no statistics derived), in order to illustrate certain phenomena with more detail or to exemplify suggestions for improvement.

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.

There was a strong consensus that wireless connected and wearable devices are associated with risks related to data protection and privacy, and protection from fraud, with only a small minority of respondents, mostly manufacturers of radio equipment, believing that the risks are low or negligible. The responses to the open questions provided some insights into stakeholders' views. They showed some consensus over the existence and nature of risks related to internet-connected radio equipment devices and wearables, but differing views over the origin of risks and the best way to address them. In that respect, mostly consumers associations and Authorities suggested that there was an inherent problem with the way that devices are designed, manufactured and sold. Some manufacturers were more inclined in suggesting that the problem is not with the devices themselves but with the service providers, i.e. it is a problem of transfer and downstream processing of data. It was in any case stressed that the problem is not limited to wireless connected devices, but also affects wired devices. As a result, the latter respondents mostly considered that the use of delegated acts under the RED was not the most appropriate solution to the problem. An alternative raised was the possibility of introducing a horizontal mandatory piece of legislation covering all types of products. This would cover minimum baseline requirements in cybersecurity to help ensure adequate security safeguards.

Open public consultation

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

- 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.

In respect of data protection and privacy, at least half of respondents were highly concerned or fairly highly concerned about all types of devices. Only 7% were not concerned at all. Devices raising most concerns were consumer devices with many functions, e.g. smartphones, laptops, smart TVs, gaming stations. Next most concerning devices were wireless devices intended for children or vulnerable adults and wearable devices for children or vulnerable adults. Devices giving least concern were commercial devices.

As regards the protection from fraud, respondents were less concerned about protection from fraud than about data protection and privacy, across all types of device. The biggest concern was raised, again regarding consumer devices with many functions, e.g. smartphones, laptops, smart TVs, gaming stations, but next biggest concern was raised regarding commercial devices (e.g. vending machines, POS terminals, public Wi-Fi). Issues that raised particular concern included the lack of requirements to force users to change ID and passwords from default settings, new security vulnerabilities which are identified on a regular basis and regular updates may not be available, location of manufacturers or operators outside the European Economic Area, volume of personal or sensitive data collected by devices used by children or vulnerable adults, lack of firmware updates.

When users experienced issues (approximately 10% of the respondents), over one-third (38%) reported that such issues had been extremely severe. Of those who experienced problems, most (62%) were deterred from buying or using such products again, at least for some time. Issues included:

- Penetration of an internet protocol camera;
- 3rd parties (potentially) listening to private conversations via wireless devices, e.g. baby monitor;
- Unknown devices trying to connect with smart televisions;
- Access to private email;
- Third party attempt to access company network and introduce viruses.

From all these consultations, it was clear that internet-connected and/or wearable radio equipment create risks to data and privacy protection and protection from fraud, with 41% of respondents to the targeted consultation labelling the risk level high (out of high, medium, low) with regard to data protection and privacy risks and 37% labelling the risk level high for risks related to the protection from fraud.

Regarding risks associated with IoT devices connected through networks, many stakeholders interviewed made the link between unsecure IoT devices and the risks posed at a network level due to Botnets. For instance, in 2016, hackers created IoT malware called Murai that scanned for insecure routers, cameras, recorders, and other IoT devices still using default passwords and then added them into a botnet network. This was then used to launch DDoS attacks on websites and Internet infrastructure, essentially making them unavailable.

The inter-linkages between poorly secured IoT devices, data protection and privacy and the risks of vulnerable devices being used for Botnet attacks was stressed by MS and consumers, but also some firms dealing with specific security matters.

The European Consumer Associations ANEC and BEUC have undertaken broader research, together with their national members, into how consumer IoT security might be enhanced. For instance, a joint position paper on Cybersecurity for Connected Products between ANEC and BEUC was adopted in 2018. This found that “most connected devices available in the EU’s Single Market are designed and manufactured without the most basic security features embedded in their software.” Furthermore, hardware vulnerabilities were also identified.

Whilst some industry manufacturing associations expressed the view that the nature of the risks has been exaggerated outside of smart toys, ICT and cybersecurity associations and cybersecurity testing houses mentioned that despite improved awareness among industry about the vulnerabilities, there are still too many products coming to the market that do not even have the most basic cybersecurity features integrated into smart products, making them vulnerable to hacking attacks and therefore, also the data on a device or that the device is able to access (from other sources or devices). A number of stakeholders commented that they believe the problem has grown much worse in the past five years, since cybersecurity has not been addressed through regulation, so therefore low-quality, non-cyber secure products remain legally sold on the European

single market. The problem had in their view been exacerbated by the trend towards smart and connected products. Manufacturers can easily include wireless (direct) or Bluetooth (indirect) connectivity to the internet as an additional product feature at very low cost, as such technologies have significantly reduced in price. Therefore, the scale of the threat has increased, due to such products' increased ubiquity.

A further observation by stakeholders (both consumer and industry associations) in terms of the nature and magnitude of risks is that there are greater concerns regarding Business to Consumer (B2C) IoT devices in ensuring data protection and privacy and protection from fraud compared with Business to Business devices (B2B). The reason for this was that unsecure B2C IoT products tend to be at the very cheap, low-quality end of the market, whereas B2B users demand encrypted products, since their own client base demands a high level of data protection and privacy. A further consideration is that many consumers have low levels of awareness and understanding about cybersecurity risks and practical know-how in terms of how to secure their device.

ANNEX 3: WHO IS AFFECTED AND HOW?

14. 1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

This initiative aims to support the policy objectives of related pieces of EU law establishing market access conditions for radio equipment. If adopted, manufacturers of equipment in scope of the initiative will have to demonstrate that specific features are present in the equipment as a condition for market access. As the Articles of the RED concerning the conformity assessment procedures will not be changed, manufacturers of equipment in scope will have to apply those procedures to demonstrate the new essential requirements concerned by the adoption of delegated acts herein discussed.

In turn, National Authorities can recall products from the market or ask for other corrective measures if these features are not present or are effective.

In order to facilitate the implementation, the Commission will launch a standardisation request, with a deadline for the delivery of harmonised standards from 3-6 months before the date of applicability of the delegated act. Preliminary work has already started.

15. 2. SUMMARY OF COSTS AND BENEFITS

I. Overview of Benefits (total for all provisions) – Option 5: Adoption of Article 3(3)(d), 3(3)(e) and 3(3)(f)		
Description	***Amount***	***Comments***
Direct benefits		
Reduction of frauds	Financial frauds to citizens could amount to **1.8 billion EUR** a year, see section 2.1.2.	This is only the part of frauds which is due to non-cash payments. This initiative is therefore expected to mitigate the risks in at least 80% of the connected products[123] currently placed on the EU market. However, as the full security concerns also other actors (e.g. service providers, operators), it is impossible to estimate the benefits with further accuracy.
Reduction of data breaches	The cost of data breaches is in the order of at least **10 billion EUR,** see section 6.6).	Not all data breaches can be prevented through this initiative, but only those run through radio equipment. This initiative is therefore expected to mitigate the risks in at least 80% of the connected products currently placed on the EU market. However, as the full security concerns also other actors (e.g.

[123] see section 2

		service providers, operators), it is impossible to estimate the benefits with further accuracy. There are however significant savings if only a small percentage can be prevented.
Reduction of DDoS	The costs of DDoS are estimated to be at least **65 billion EUR**.	Not all these incidents can be prevented through this initiative, but only those run through radio equipment. This initiative is therefore expected to mitigate the risks in at least 80% of the connected products currently placed on the EU market. However, as the full security concerns also other actors (e.g. service providers, operators), it is impossible to estimate the benefits with further accuracy. There are however significant savings if only a small percentage can be prevented.
Prospective business opportunities in a secure DSM	This accounts approximately at least for 36 billion EUR in 10 years (**3.6 billion a year** on average), only for 5G-related technologies, see section 2.3.	The precondition of this benefit is to have a secure DSM. This initiative will contribute to it, proportionally to the covered equipment and the risks. Certain wired equipment, accounting approximately for 20% of the total connected equipment, is not in scope and may require further initiatives.
Citizens' trust in the DSM	This is not quantifiable, but the lack of trust of citizens can undermine –or delay– all the DSM development.	This initiative will contribute to build citizens' trust in the DSM, proportionally to the covered equipment and the risks. Certain wired equipment, accounting approximately for 20% of the total connected equipment, is not in scope and may require further initiatives.
Increase of citizens privacy / reduction of identity theft	This is not quantifiable, as it concerns the protection of fundamental rights	This initiative will contribute to increase citizens' privacy, proportionally to the covered equipment and the risks. Certain wired equipment, accounting approximately for 20% of the total connected equipment, is not in scope and may require further initiatives.
Improved functioning of the Internal Market by ensuring that a level playing field is maintained without the emergence of national divergent legislation	This is not quantifiable, but it is expected that, if national legislation is adopted, the costs for manufacturers will be at least the same as under Option 5. Possible divergence of the national initiatives will make the costs for manufacturers even higher.	This initiative will contribute to an improved functioning of the Internal Market, proportionally to the equipment in scope. Certain wired equipment, accounting approximately for 20% of the total connected

		equipment, is not in scope and may require further initiatives.
Competitiveness of EU industry in the digital economy, establishment of a level playing field	This is not quantifiable, but diligent manufacturers that have spent resources to ensure security of their products – also following the provisions in the GDPR – may not have sufficient incentives to continue to do so, in the absence of enforcement.	This initiative will contribute to establish a level playing field for the equipment in scope.
Indirect benefits		
Reduction of fraudulent and criminal consequences of personal data thefts	This includes any costs related to responding to these crimes (e.g. police and victim services etc).	Not all these incidents can be prevented through this initiative but only those run through radio equipment, which accounts for approximately 80% of all connected equipment.
Increased protection of networks	Operators of networks will benefit from more secure equipment, which is often the "weakest link", which can result in reduced incidents and consequently savings.	-
Prevention of reputational damage	Reputational damage can account up to 25% of the value of the enterprise/firm. Ensuring a higher level of security can help prevent this damage, at least in part.	-

Notes:

- *As in section 2.4, the COVID crisis may have magnified the costs for manufacturers and the benefits for the society, although a quantitative estimate is not possible at the point of preparing this IA (September 2020)*
- *Estimates are relative to the baseline for the preferred option as a whole*
- *Aggregated costs for the manufacturing sector could not be estimated, not being possible to estimate the number of models of radio equipment placed annually on the EU market.*

II. Overview of costs – Preferred option							
		Citizens/Consumers		Businesses		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Action (a)	Direct costs	N/A	N/A	Costs to ensure a "security by design", which has not yet been sustained under the GDPR	Costs for testing, 5k-50k EUR per equipment type, although some of these costs have a high BaU – see table 2 – and should have already been incurred under the GDPR	N/A	Costs for additional testing, 5k-10k EUR per equipment type (model), with an aggregate cost around 40 additional million EUR with respect to the baseline.
	Indirect costs	N/A	Potentially higher prices for equipment that consumers are ready to afford to get more secure products. See table 3 for details	N/A	N/A	N/A	N/A

Notes:

- *As in section 2.4, the COVID crisis may have magnified the costs for manufacturers and the benefits for the society, although a quantitative estimate is not possible at the point of preparing this IA (February 2021)*
- *Estimates are relative to the baseline for the preferred option as a whole*

- *Aggregated costs for the manufacturing sector could not be estimated, not being possible to estimate the number of models of radio equipment placed annually on the EU market.*

ANNEX 4: ANALYTICAL METHODS

The impact assessment study placed a strong emphasis on stakeholder consultations. A stakeholder consultation strategy was developed consisting of a combination of interviews and two online questionnaires, an OPC questionnaire and online questionnaire for targeted stakeholders. The Expert Group on Radio Equipment was consulted regularly, as well as the ADCO RED.

Feedback received from stakeholders were complemented through desk research. Efforts were spent to get reliable quantitative data. In many cases stakeholders could not provide precise costs, mentioning for instance that costs would be a function of the technical solutions in standards and harmonised standards. As well, it was not possible to retrieve with precision which costs had been already incurred to comply with current legislation (e.g. GDPR).

ANNEX 5: APPLICABLE DELEGATED ACTS

Article 50 of the RED provides that references to the repealed Directive 1999/5/EC (R&TTED)[124] shall be construed as references to this Directive (i.e. the RED). Any Commission Decisions, adopted under the R&TTED, remain applicable under the RED to the extent that they are not incompatible with the RED, until they are repealed. This is the case of the following acts:

- Commission Decision 2000/637/EC of 22 September 2000 on the application of Article 3(3)(e) of Directive 1999/5/EC to radio equipment covered by the regional arrangement concerning the radiotelephone service on inland waterways;
- Commission Decision 2001/148/EC of 21 February 2001 on the application of Article 3(3)(e) of Directive 1999/5/EC to avalanche beacons;
- Commission Decision 2013/638/EC of 12 August 2013 on essential requirements relating to marine radio communication equipment which is intended to be used on non-SOLAS vessels and to participate in the Global Maritime Distress and Safety System (GMDSS);
- Commission Decision 2005/53/EC of 25 January 2005 on the application of Article 3(3)(e) of Directive 1999/5/EC of the European Parliament and of the Council to radio equipment intended to participate in the Automatic Identification System (AIS);
- Commission Decision 2005/631/EC of 29 August 2005 concerning essential requirements as referred to in Directive 1999/5/EC of the European Parliament and of the Council ensuring access of Cospas-Sarsat locator beacons to emergency services.
- Moreover, there is also the Commission Delegated Regulation (EU) 2019/320 of 12 December 2018 supplementing of 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)(g) of that Directive in order to ensure caller location in emergency communications from mobile devices.

[124] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, Official Journal L 091, 07/04/1999 P. 0010 - 0028

ANNEX 6: COHERENCY MAPPING – RELATED PIECES OF EU LAW

The General Data Protection Regulation (EU) 2016/679 (GDPR) and the Directive on privacy and electronic communications (Directive 2002/58/EC, "ePD"[125]), set forth **rules on data protection and privacy protection**. However, these rules are addressed to controllers and processors of personal data, not to device manufacturers as such. That said, recital 78 GDPR encourages manufacturers to take its requirements into account. The GDPR (Art. 12) already provides that any information addressed specifically to a child will need to be adapted to be easily accessible, using clear and plain language. Fines may be issued under the GDPR, but data protection authorities can conduct enforcement activities such as instituting legal proceedings and issuing fines, whilst market surveillance authorities cannot remove insecure products from the market. In addition, other rules of the GDPR are also relevant in this context, such as Article 25, which mandates data protection by default and by design and Article 32, which mandates security of processing. Under the GDPR, consent[126] has to be a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Art. 4(11)). It is worth noting that the definition of consent under the GDPR also applies for the purpose of obtaining consent under the ePD, in particular as concerns the placing of cookies and other online trackers. According to the principles of the GDPR (Article 5) personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

A delegated act pursuant Article 3(3)(e) of the RED would allow the essential requirement of safeguards to ensure that the personal data and privacy are protected to be demonstrated a product in question can be placed on the market, also in line with recital 10 of the ePD[127].

The "Cybersecurity Act"[128] (CSA) **establishes voluntary certification scheme** for showing cybersecurity resilience. Subject to future stakeholder consultations, a relevant certification scheme may be established

[125] Currently under revision
[126] Article 7 of the Regulation
[127] *"[…] It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (7) will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market".*
[128] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

with cybersecurity requirements related to the objectives of the delegated act i.e. safeguarding data protection, privacy and ensuring protection from fraud. It is obvious that certain baseline requirements in relevant schemes will have to be incorporated in the RED harmonised standards so to achieve both the objectives of (i) mandating minimum requirements for the market access of equipment (RED) and (ii) allow consumers and users to ascertain between different levels of cyber-protection (CSA).

The "Non-cash payment Directive"[129] **defines which behaviours are to be considered criminal with respect to frauds**. These extend beyond the 'fraudulent use' and span to a whole set of offences 'related to' fraudulent use, where inspiration can be found to identify which kind of protection should be warranted. Identification of different forms of behaviours requiring criminalisation in relation to fraud and counterfeiting of non-cash means of payments: offences related to payment instruments (e.g. theft, counterfeiting, falsification, receiving or selling fraudulent use stolen or counterfeited payment instruments, use of a stolen or counterfeited payment instrument); offences related to computers (i.e. performing or causing a transfer of money by introducing, altering, deleting or suppressing computer data or by interfering with the functioning of a computer programme or system); offences related to specifically adapted devices (e.g. fraudulent making, receiving, obtaining, sale or transfer to another person or possession of instruments, articles, computer programmes and any other means peculiarly adapted for the commission of counterfeiting or falsification of a payment instrument).

The Directive 2013/40/EU on attacks against information systems (the 'cyberattack directive') aims to prevent cyber-attacks, by approximating Member State's definitions of cybercrime offences, setting minimum maximum penalties and providing a framework for the exchange of information on these crimes between Member States, and for the collection of statistical information. Amongst other things, the Directive provides for criminal liability for illegal access to information systems, illegal interference with systems and data, illegal interception and the illegal distribution of tools to commit such offences, particularly large-scale attacks either affecting a significant number of information systems (e.g. "botnets"), causing serious damage, aiming at critical infrastructure systems or misusing the personal data of another person ("ID fraud"). Information systems is defined broadly in the Directive to ensure a technology independent and future-proof approach. The definition encompasses "*a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance*".

Directive (EU) 2016/1148 (the **NIS Directive**) concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) is the first horizontal internal market instrument aimed at improving the resilience of networks and systems in the Union against cybersecurity risks. It has introduced concrete measures building cybersecurity capabilities and mitigating growing threats to network and information systems used to provide essential services in seven sectors for the EU economy and society, which rely heavily on ICT (energy, transport, banking, financial market infrastructures, health, water supply and distribution and digital infrastructure), as well as for key digital service providers (online marketplaces, online search engines and cloud computing services). The Directive obliges these undertakings to report major security incidents to the competent national authorities. It therefore ensures (i) Member States' preparedness, (ii) effective operational cooperation on specific cybersecurity incidents and sharing

[129] 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 https://eur-lex.europa.eu/eli/dir/2019/713/oj

information about risks, (iii) appropriate security measures and notification of serious incidents. The security of networks is, however, also depending on the used terminal equipment and hence securing the equipment is a complementary needed step to support the security of infrastructures. For this reason Article 3(3)(d) will ensure that at least radio terminal equipment contains mandatory requirements in support and in complement to the EU policy objectives. The Commission announced in its Work Programme 2020 that it would review the NIS Directive by the end of 2020. This would advance the deadline foreseen under Article 23(2) of the Directive, according to which, the Commission shall review the functioning of the Directive and report to the European Parliament and the Council by 9 May 2021. This is further justified by the sudden increase in the dependence on information technology during the COVID 19 crisis.

The Regulation (EU) No 910/2014 of the European Parliament and of the Council lays down rules to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities. It ensure that individuals and businesses can use their national electronic identification schemes for online access to public services in other EU Member States through establishing interoperability and enforcing mutual recognition. In order to support mutual recognition of national electronic identification schemes under eIDAS, Implementing Regulation 2015/1502 defines three levels of assurance - low, substantial and high – and establishes minimum technology-neutral requirements, standards and procedures to achieve compliance with the respective security requirements.

The activation of one or more delegated acts pursuant Articles 3(3)(d), 3(3)(e) and/or 3(3)(f) of the RED, will also entail that, if Member States identify a radio-connected product presenting a serious risk related to personal data, privacy or fraud, a notification should be submitted through **the Rapid Alert System for dangerous non-food products (RAPEX).** As it is established in Articles 1, 16, 20 and 22 of Regulation 765/2008, market surveillance authorities should ensure that products fulfil the specific requirements established in EU legislation relating to technology, health and safety, environment or any other aspect of public interest protection (which in this case would be the protection of personal data, privacy and fraud). In addition to protecting consumers, the notification through the Rapid Alert System of radio-connected products not respecting the essential requirements established on the delegate act((s) will also ensure that the free movement of these products in the Single Market is not restricted to any extent greater than what is allowed under EU legislation.

The Regulation (EU) 2019/1020 on market surveillance and compliance of products supports fairer internal market for goods, through fostering more cooperation among national market surveillance authorities. This will include sharing information about illegal products and ongoing investigations so that authorities can take effective action against non-compliant products.

ANNEX 7: CASE STUDIES

In this section we report two case studies which exemplify the costs in specific industrial sectors. Other case studies, which have a reduced information have been reported in Annex 8 of the Impact assessment study for this initiative[130].

Mini case study - Costs of compliance of possible activation of delegated Acts under Articles 3(3)(e) and 3(3)(f) of the RED for the lawnmowers industry

Sector- Garden equipment.

Lawnmowers have traditionally been an offline simple product subject to core industrial product legislation, such as the Directives 2014/30/EU and 2014/35/EU. However, in common with other household and gardening electrical appliances and tools, there is a growing tendency towards integrating connectivity capabilities in such products. This is partly to facilitate data communications from the machine to the manufacturer about performance, but also due to changing market and consumer trends, such as growing interest in, and commonality of robotic lawnmowers. This requires connectivity, for instance, when the lawnmower is controlled by the consumer via an app.

Security vulnerabilities– level of risk: The risks associated with lawnmowers from a cybersecurity perspective can be assessed at two levels, firstly product-level risks, and secondly, generic risks when the product is connected to the internet via a (home) network. Regarding product-level risks, lawnmowers were seen by the interviewee as traditionally being a low-tech product, but such products now often have internet connectivity. It was argued however that the risks should not be over-estimated, since the type of information and data being transferred back to the manufacturer is non-personal data, and more to do with the lawnmower's technical performance.

Implications of the possible activation of delegated Acts under Articles 3(3)(e) and 3(3)(f): If a combination of encryption and authentication were to be required, this would imply a certain level of costs, since presently many of the chips used in lawnmowers are unsecure, in that they do not have encryption or require authentication. Whilst recognising that cybersecurity could be improved, the industry stakeholders interviewed advocated relying on a voluntary, industry-led approach on the basis that imposing mandatory requirements relating to the use of passwords and encryption may be overkill for many IoT products.

However, a counterpoint was that the main risks could rather be associated with how lower-tech products are internet-connected. The home network itself could pose a greater risk of a data security breach than the product itself. A challenge however is that lower-tech products with connectivity through cheap components that do not have encryption or require authentication could be the weakest link in the chain.

Administrative and substantive costs of compliance (regulatory approach):
The interviewee noted that there would be additional costs if mandatory requirements were to be

[130] https://ec.europa.eu/docsroom/documents/40763

introduced relating to data protection and privacy for lawnmowers. It was estimated that:

- Administrative compliance costs were estimated at 25,000 EUR per product
- The additional costs could be up to 3 EUR / unit more expensive compared with a non-secured lawnmower product with cheap Wi-Fi connectivity.
- Integrated encryption into the Central Processing Unit (CPU) would require changes to the electronics and additional technical support. This could result in extra costs of up to 10 EUR/ unit.
- Turning to substantive costs, the R&D costs are estimated at 100,000 EUR – strong authentication for use. 100,000 EUR – back-end development costs.

Market size and structure: the market structure is important, since this would affect the industry's ability to absorb the compliance costs of integrating costs such as those above. The industry **is comprised of some large players and some SMEs. The largest market players are both European and global. There were concerns that more expensive products of European manufacturers might seem less attractive to consumers and users, if they are required to follow additional EU legislative requirements on cybersecurity compared with their global competitors, but equally, this could also be used for marketing purposes to differentiate from the competition.**

Views on alternative means of strengthen cybersecurity in the industry: If additional essential requirements are added, this was seen as potentially adding quite a lot of cost. It was suggested that an alternative could be to address the risks through existing EU legislation treating cybersecurity in industrial products as a horizontal theme to be addressed through the GDPR and the voluntary Cybersecurity Act. Cybersecurity needs to be mentioned in many different pieces of EU legislation applicable to industrial products, not only in the RED in their view. There was a concern about the legal consistency and coherence of the EU legal framework if IoT-specific requirements were to be introduced only applicable to products falling within the scope of the RED, this would mean that unconnected lawnmowers would not be subject to additional requirements, which could penalise innovation, with only more advanced, connected products subject to additional requirements. An argument against this however is that unconnected products do not pose the same magnitude of risk from a cybersecurity perspective precisely because they are not connected.

In conclusion, the increase of costs (up to 10 EUR/unit) in connected lawnmower appear to be a bearable fraction of the overall cost of the product, which is in the order of some hundred euros. These increase in costs are based on the assumption that one expensive technology will be used, without taking into account different mitigating factors, as for instance (i) the availability of equivalent but less costly technologies or (ii) the reduction of costs due to scale production, when/if all "internet-connected radio equipment" have to use more secure technologies or (iii) the fact that certain costs can be mitigated through the distribution of the requirements through the value chain.

Source: desk research, interview with industry association who provided feedback from one of their members in the gardening equipment industry, specifically lawnmowers.

Mini case study - Showing estimated costs for routers

Market size/ structure:	The current global market for routers is expected to grow at a CAGR of 16.9% over the next five years, and will grow from 810 million US$ in 2019 to 2070 million US$ in 2024[131]. Other market research reports estimate the market size to be as much as 10 times higher by 2024. The global market for routers was estimated in a second study at USD 23 billion by 2024 [132] which is considerably higher, illustrating the challenges of getting an accurate picture on market size and structure. Data from Tech4i2 estimated market size in terms of routers in Europe is expected to be 290m by 2030 in the EU-28 MS, an increase from 244m in 2020.
Key demand drivers to 2030	Increased usage of Gigabit high-speed internet, driven by increasing demand for internet-connected radio equipment, an expansion in industrial and consumer IoT and in cloud-based networking.
Type of costs:	Internal and external testing costs related to software development to check security features.
Type of enterprises interviewed:	Medium-sized and large producers.
Analysis of costs:	Example from the medium-sized producer interviewed. Costs for one manufacturer for one product (internal, external) • Internal security testing costs – €60,000. Workings: ▪ Product development process lasts 6 months tying up 2 full-time employees on security matters. In practice, this would include 5-6 people only part of their time e.g. product engineers doing the testing, managers dealing with new product development and launch, legal staff. • External security testing costs • Before a new router is placed on the European market, following internal testing, the manufacturer typically requires 5-6 external software developers and engineers to check the software code and the product's systems architecture, with each person making about 1 month's input each. • The day rate for software developer with knowledge of quality assurance in coding - €1,500 / day. Over one month, total cost - €1500 X 21 days X 5.5 coders = €173.250. • But the majority of costs relate to testing software against different product performance parameters, while a smaller proportion relates to

[131] Router Market 2019 Research report https://www.360researchreports.com/enquiry/request-sample/13814132
[132] Source - global industry analysts. https://www.strategyr.com/MCP-1750.asp

	security. Working assumption – 40% of costs relate to security, 60% to checking performance and product functionality beyond security, hence €69.300 (€173.250 X 40%) for security alone. Assumptions underpinning extrapolation: • Estimated 44 major router manufacturers selling products in Europe, according to research by our study team (mapping of router manufacturers undertaken by study team). • Each router manufacturer brings estimated circa 3 new router products / year to the market (consumer segment). • €69.300 cost benchmark for a router X 44 (total n manufacturers) X 3 n products on av. brought to market annually. €9.147.600 is the total estimated annual cost of third-party security testing for routers in Europe. • Internal costs - €60.000 X 44 manufacturers X 3 products brought to market annually est. = €7.920.000. • Total testing costs per year (internal and external) are - €9.147.600 + €7.920.000 = €17.067.600. • Assumptions on number of devices in the European market: presently, there are 240 million devices in total on the market, and an expected 290 million routers by 2030 (source – Tech4i2, see Annex 5 with projections on the number of radio devices), • Annual sales could be 20% of this total figure (on the basis that users replace their router once every 5 years), equivalent to 48 million routers purchased per year. • This implies testing costs of €17.067.600 testing costs total / 48 million routers or €0.355 per router. • Greater costs would however be incurred through the introduction of baseline security requirements, e.g. if specific new technical standards are brought in requiring particular security features. However, as the specific types of requirements are not yet known, this was not possible to quantify.
Estimated BaU costs:	70-80%. If the RED delegated acts were to be introduced, many of the costs are assumed to be BaU as the router manufacturer's wholesale clients already demand support. The firm concerned is already testing products extensively before they are placed on the market. The rationale for this is reputation and risk management as rather than selling directly to the public through retailers, they sell wholesale. So therefore, very high BaU costs might be assumed, as the firm is already testing product security in great detail before placing product on the market. More broadly across routers as a whole, the costs of integrating some additional features - whilst difficult to quantify - such as Wi-Fi Protected Access II (WPA2) Encryption, Guest Network Access, Built-in Firewalls, and eliminating easy-to-guess passwords and user names and passwords by default could be discounted as they have either high BaU costs (WPA2 Encryption, Guest Network Access, Built-

	in Firewalls) or require implementing common sense changes in security practices (e.g. avoiding the use of default passwords).
Conclusions	Overall, the costs appear to be proportionate. The testing costs, whilst imposing a degree of administrative costs, are manageable for medium and large-sized producers that dominate the wireless router market. Our assessment shows that the costs per router of testing is only €0.355 per device. However, it should be noted that this excludes any substantive compliance costs due to having to integrate particular security features as the costs would be strongly dependent on what types of technical standards and which features are required.

Source: Commission's contractor – analysis of results from interview programme, desk research, and data estimates on market size/ structure

Glossary

Term or acronym	*Meaning or definition*
ADCO RED	Administrative Cooperation Group of Market Surveillance Authorities of the Radio Equipment Directive
ANEC	European Association for the Co-ordination of Consumer Representation in Standardisation
BaU	Business as Usual costs (costs that could be incurred anyway by business regardless as to whether there is new legislation).
B2B/C	Business to Business/Consumers
BEUC	Bureau Européen des Unions de Consommateurs
CAGR	Compound Annual Growth Rate
CBA	Cost-Benefit Analysis
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CNP	Card Not Present
CPU	Central Processing Unit
CSA	Cybersecurity Act
DDoS	Distributed Denial of Service
DSM	Digital Single Market
ePD	ePrivacy Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in Electronic Communications)
EDPB	European Data Protection Board
eIDAS	Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market
ENISA	European Network and Information Security Agency
ESO	European Standardisation Organisation
GDPR	General Data Protection Regulation (EU) 2016/679 (GDPR)
GNSS	Global Navigation Satellite System
IA	Impact Assessment
ICT	Information and Communication Technology
IoT	Internet of Things
IT	Information Technology
IP	Internet Protocol
ITU	International Telecommunication Union
MS	Member State
MSA	Market Surveillance Authority
NACE	Nomenclature statistique des Activités économiques dans la Communauté Européenne
NFC	Near-Field Communications
NIS	Network and Information Systems
NLF	New Legislative Framework
OPC	Open Public Consultation
RED	Radio Equipment Directive (2014/53/EU)
RFID	Radio Frequency IDentification
RLAN	Radio Local Area Network
SEPA	Single Euro Payments Area
SME	Small and Medium Enterprise
TCAM	Telecommunications Conformity Assessment and Market Surveillance
TFEU	Treaty of Functioning of the European Union
WPA	Wi-Fi Protected Access
WTP	Willingness to Pay