Final Report

Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment

716/PP/GRO/IMA/18/1133/10768 IMPLEMENTING FRAMEWORK CONTRACT 575/PP/2016/FC

April, 2020

Lead author: Mark Whittle (CSES)

Supporting authors: James Eager (CSES), Eugénie Lale-Demoz (CSES), Giuseppe Maio (CSES associate, Trilateral Research), Professor Paul Foley (Tech4i2) and Richard Potter (Tech4i2).

QA review by: External expert, Dr. Marie-Helen Maras

Centre for Strategy & Evaluation Services LLP
Westering House
17 Coombe Road
Otford, Kent TN14 5RJ
United Kingdom
E: enquiries@cses.co.uk
T: +44 (0) 1959 525122

Contents

1. Introduction 1

1.1 Study objectives and scope ... 1

1.2 Methodology and Analytical framework ... 1

1.2.1 Methodological approach ... 1

1.2.2 Results of the stakeholder consultations ... 2

1.2.3 Analytical framework ... 3

1.3 Definitions ... 5

1.3.1 Definition of the Internet of Things ... 5

1.3.2 Definition of personal data, data protection and privacy ... 5

1.3.3 Definition of data protection by design and default ... 8

1.3.4 Definition of protection from fraud ... 9

1.3.5 Definition of security by design and default ... 10

1.4 Structure of the final report ... 11

2. Background and policy context 13

2.1 Background and policy context ... 13

2.1.1 Legal framework – an overview of the Radio Equipment Directive ... 13

2.1.2 Broader study context ... 14

3. Problem definition 17

3.1 Key trends and review of market size and structure for connected radio equipment ... 17

3.1.1 Trends in radio equipment products ... 17

3.1.2 Market size and structure ... 20

3.2 Conceptualisation of radio equipment security risks, consequences and solutions ... 22

3.2.1 Conceptualisation of security breaches and their impacts ... 22

3.2.2 Security breaches and solutions ... 24

3.2.3 Solutions: Preventing breaches ... 24

3.2.4 Consequences of security breaches ... 26

3.2.5 Conceptualisation of data misuse and its impact ... 27

3.3 Analysis of existing EU legislation and regulatory gaps ... 28

3.3.1 Mapping of relevant EU legislation ... 28

3.3.2 Legal requirements in relation to data collection and processing and the ethical dimension of data and information use by manufacturers ... 38

3.3.3 Data protection and privacy in the context of connected radio equipment and wearables ... 41

3.3.4 Protection from fraud in the context of connected radio equipment and wearables ... 44

3.3.5 National and international developments in addressing the security vulnerabilities in connected RE products/ devices and wearables 47

3.3.6 National developments in the EU and third countries 48

3.3.7 Regulatory developments in the US 49

4. Assessment of risks, vulnerabilities and consequences of breaches 52

4.1 Connected radio equipment – introductory assessment of risks and vulnerabilities....52

4.1.1 Stakeholder views and observations 53

4.2 Synthesis assessment of security vulnerabilities and technical solutions in internet connected radio equipment products....58

4.2.1 Security vulnerabilities in internet-connected RE products 58

4.2.2 Analysis of security vulnerabilities by product, risk assessment and degree of impacts 66

4.2.3 Technical solutions 72

4.2.4 Synthesis assessment - issues relating to the collection and processing of personal data....84

4.3 Stakeholders affected by security risks in connected radio equipment products 91

4.4 Locational factors and risks 92

5. Analysis of Policy Options, Impacts and CBA 93

5.1 Analysis of policy options 93

5.1.1 Strategic policy considerations – strengthening the security of internet-connected RE products....93

5.1.2 Definition of policy options 93

5.1.3 Policy Option 0 - Status quo: reliance on existing EU legislation 95

5.1.4 Policy Option 1 – A voluntary approach....100

5.1.5 Policy Option 2, 3 and 4 – A regulatory approach....107

5.1.6 Policy Option 5 – a horizontal piece of legislation on cybersecurity 115

5.2 Analysis of Impacts....116

5.2.1 Economic impacts....117

5.2.2 Social impacts 119

5.2.3 Environmental impacts....120

5.2.4 Unintended consequences and impacts. 121

5.2.5 Overall findings - impacts 122

5.3 Cost-benefit analysis (“CBA”) of the Policy Options 123

5.3.1 Introduction to the CBA and methodology 123

5.3.2 Challenges in undertaking the CBA 124

5.3.3 Compliance costs types 126

5.3.4 Quantification of the costs and benefits of existing EU legislation (Option 0) 127

5.3.5 Stakeholder feedback on the costs of activating the delegated acts....128

5.3.6 Administrative costs - online survey findings 128
5.3.7 Administrative burdens 140
5.3.8 Substantive compliance costs 140
5.3.9 Business as Usual (BaU) costs 148
5.3.10 Compliance costs for large firms and SMEs 149
5.3.11 The costs of data breaches 150
5.3.12 Benefits of activating the delegated acts 156
5.3.13 Summary findings - the quantification of costs 161

6. Conclusions 166

6.1 Conclusions and recommendations 166
6.1.1 Penetration of connected RE devices in European households 166
6.1.2 Security vulnerabilities in connected RE products and wearables 166
6.1.3 Extent of protection in existing EU legislation and analysis of regulatory gaps 168
6.1.4 The collection of personal data from connected RE products and wearables and privacy implications 170
6.1.5 Analysis of stakeholder consultation feedback 172
6.1.6 Analysis of policy options, impacts and CBA: 173
6.1.7 Impacts 178
6.1.8 Cost-benefit assessment (CBA) 178
6.2 Recommendations 181
6.2.1 Recommendations from the IA study 181
6.2.2 Further strategic recommendations 182

Annex 1 - Bibliography 185

Annex 2 – Key study issues: an analytical framework 203

Annex 3 - Interviews conducted 206

Annex 4 – Checklist data protection and privacy by design and default 207

Annex 5 – Forecasts for internet-connected radio equipment 208

Annex 6 – Analysis of targeted consultation responses 209

Annex 7 – Analysis of OPC consultation responses 210

Annex 8 – Product-based case studies 211

Tables

Table 1.1: Steps in the Impact Assessment process ... 3
Table 1.2: Art. 4 Definitions of the GDPR points 1-5 ... 6
Table 2.1: Delegated Acts possible under Article 3(3e) and 3(3f) ... 13
Table 2.2: IoT Units installed base by category (millions of units) ... 15
Table 3.1: Categorisation of radio equipment ... 18
Table 3.2: The main NACE classes that produce radio equipment ... 20
Table 3.3: The main NACE classes that produce components for radio equipment ... 21
Table 3.4: Statistics for the main radio device NACE groups and classes 2016 ... 21
Table 3.5: Statistics for key components for radio device NACE groups and classes 2016 ... 22
Table 3.6: Analysis of existing EU legislation - relevance to strengthening security (data protection and privacy and protection from fraud) ... 29
Table 4.1: Vulnerability of radio equipment to different security breaches and consequences ... 52
Table 4.2: Cross-comparative summary of security vulnerabilities of radio equipment ... 68
Table 4.3: List of technical solutions prepared by experts from CEN/CLC/JTC 13/WG 6. ... 75
Table 4.4: Types of personal and non-personal data ... 84
Table 5.1: Analysis of data collected by policy option ... 93
Table 5.2: Overview of the advantages and disadvantages of Option 5 ... 116
Table 5.3: Inception impact assessment report ... 116
Table 5.4: Typology of administrative costs ... 128
Table 5.5: Level of administrative cost associated with different compliance processes ... 130
Table 5.7: Examples of the costs of third-party testing for economic operators ... 134
Table 5.8: Routers - case study showing estimated costs of security testing prior to product launch (current situation) ... 136
Table 5.9: Examples of the costs of testing for market surveillance authorities to test internet-connected RE devices and products ... 140
Table 5.10: Substantive compliance costs: making a product data-encrypted to ensure higher levels of data protection and privacy ... 144
Table 5.11: Article 25 and 35, GDPR ... 152
Table 5.12: Estimated benefits from enhanced consumer trust and WTP consumer preferences ... 160

Figures

Figure 1.1: Methodological approach ... 2
Figure 3.1: Forecasts for Radio equipment devices in use 2015 to 2030 (excluding RFID and medical devices) ... 19
Figure 3.2: Conceptualisation of radio equipment security breaches and consequences ... 23
Figure 5.1: Administrative burden of new regulatory requirements (data protection & privacy) ... 129
Figure 5.2: Administrative burden of new regulatory requirements (fraud) ... 129
Figure 5.3: Types of administrative burden incurred by firms ... 130
Figure 5.4: Incidence of substantive compliance costs ... 142
Figure 5.5: Research and development costs to redesign chipsets or components ... 142
Figure 5.6: Research and development costs to redesign products ... 143
Figure 5.7: Average costs of data breaches globally – for companies ... 153
Figure 5.8: Behavioural experiment – WTP for IoT security labelling for four categories of internet-connected RE ... 159
Figure 5.9: Willingness to Pay (% of product price) ... 160

Boxes

Box 3.1: Case study insight: Vulnerability monitoring and documentation 26
Box 3.2: GDPR – considerations as to how far the legislation is fit for purpose to regulate data protection and privacy in an IoT context 35
Box 3.3: Fraud in the context of internet-connected RE devices: Examples 45
Box 4.1: Case study 1 - Security vulnerabilities in internet-connected toys.. 56
Box 4.2: Mobile phone hacking via third party app's 61
Box 4.3: Evolution in wireless security protocols (including encryption and authentication technologies) 63
Box 4.4: Weaknesses in the WPA2 protocol 64
Box 4.5: Typology of authentication and encryption 74
Box 4.6: Case study 3- Review of existing Technical Solutions to Strengthen Consumer IoT security (ETSI TS 103 645) 78
Box 5.1: Case study - Voluntary codes of practice to strengthen the security of internet-connected RE and wearables. 102
Box 5.2: Sectoral Codes under the GDPR, Art. 40(2). 107
Box 5.3: Case study - The administrative and substantive costs of compliance of integrating cybersecurity requirements into connected IoT products: the case of lawn mowers. 131
Box 5.4: Insight into the cost drivers of security in smart toys – uncertainties in quantification. 145
Box 5.5: The benefits and costs of encryption – avoiding a prescriptive approach to ensure costs are proportionate 146

List of acronyms

Acronyms	Full meaning
AI	Artificial intelligence
BaU	Business as Usual costs (costs that could be incurred anyway by business regardless as to whether there is new legislation).
B2B	Business-to-business
B2C	Business-to-consumer
CBA	Cost-Benefit Analysis
CoP	Code of Practice
CSA	Cybersecurity Act
DA(s)	Delegated Act(s)
DCMS	Department for Digital Culture, Media and Sport
DDoS	Distributed denial of service (attacks that can be mounted at the network level using networks of hacked individual IoT security devices).
DPbDD	Data protection by design and default
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment (process that helps organisations identify and minimise risks that result from data processing. DPIAs are usually undertaken when introducing new data processing processes, systems or technologies).
DPO	Data Protection Officer (within an organisation, manufacturer or other economic operator)
DSM	Digital Single Market
EO	Economic operators
ePD	ePrivacy Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in Electronic Communications)
ePR	ePrivacy Regulation (Proposal for a Regulation of the EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications. COM/2017/010 final - 2017/03 (COD)
ENISA	European Network and Information Security Agency
EDPB	European Data Protection Board
ETSI	European Telecommunication Standards Institute
GDPR	General Data Protection Regulation (EU) 2016/679 (GDPR)
GVC	Global Value Chains
IA	Impact Assessment
IoT	Internet of Things. IoT system architecture is generally divided into three layers: the perception layer, the network layer and service layer (or application layer)
IoTSF	Internet of Things Security Foundation
MSA	Market Surveillance Authority
NACE	*Nomenclature des Activités Économiques dans la Communauté Européenne)* is a European industry standard classification system similar in function to Standard Industry Classification (SIC) and North American Industry Classification System (NAICS) for classifying business activities.
NCSC	National Cyber Security Centre UK
NFC	Near-Field Communications
ODM	Original Design Manufacturer
OEM	Original Equipment Manufacturer

Acronyms	Full meaning
OPC	Open Public Consultation
OS	Operating System
PO	Policy option(s)
RE	Radio Equipment
RE EG	Radio Equipment Expert Group
RED	Radio Equipment Directive (2014/53/EU)
RED ADCO	Radio Equipment Directive Administrative Cooperation Group
RFID	Radio-frequency identification
SBS	Eurostat's Structural Business Statistics (SBS), which shed light on relevant classes of connected Radio Equipment and Wearables.
SSL	Secure Sockets Layer
T&C	Terms and conditions
TEE	Trusted Execution Environment - a secure area of a main processor.
TLS	Transport Layer Security
TUIs	Trusted User Interfaces for securing critical mobile apps.
TS	Technical Standard
WLAN	Wireless local area network
WTP	Willingness to Pay – economics concept relating to the maximum amount that consumers are willing to pay for internet- connected radio equipment e.g. for products with and without security features.

1. Introduction

This document contains the final report for the study to undertake an *"Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment".* The study was contracted through Framework Contract 575/PP/2016/FC for DG GROW, and was led by CSES (supported by specialist partners Tech4i2).

1.1 Study objectives and scope

This study supports the development of an Impact Assessment ("IA") by the European Commission ("EC") to review some of the (potential future) essential requirements mentioned in the Radio Equipment Directive 2014/53/EU ("RED"), which were set out in a series of delegated acts[1] under Article 3(3) of the RED. Specifically, the study objectives are to:

- verify whether a minimum level of "baseline" security measures should be integrated as a legislative requirement into the RED through the activation of either one or both delegated acts pursuant to Art. 3(3)(e) and 3(3)(f) as a *"condition for market access for internet-connected radio equipment and wearable radio equipment";*
- consider the extent to which current market access conditions are acceptable without regulation, or whether such regulation could be needed at some point in the future; and to
- identify the specific classes of radio equipment that could be covered through the delegated acts which could be activated under the above Articles of the RED, i.e. whether these should be made applicable across all classes of internet-connected radio equipment and connected wearable radio equipment, or confined to specific categories of equipment.

The study assignment was undertaken between April 2019 and February 2020.

1.2 Methodology and Analytical framework

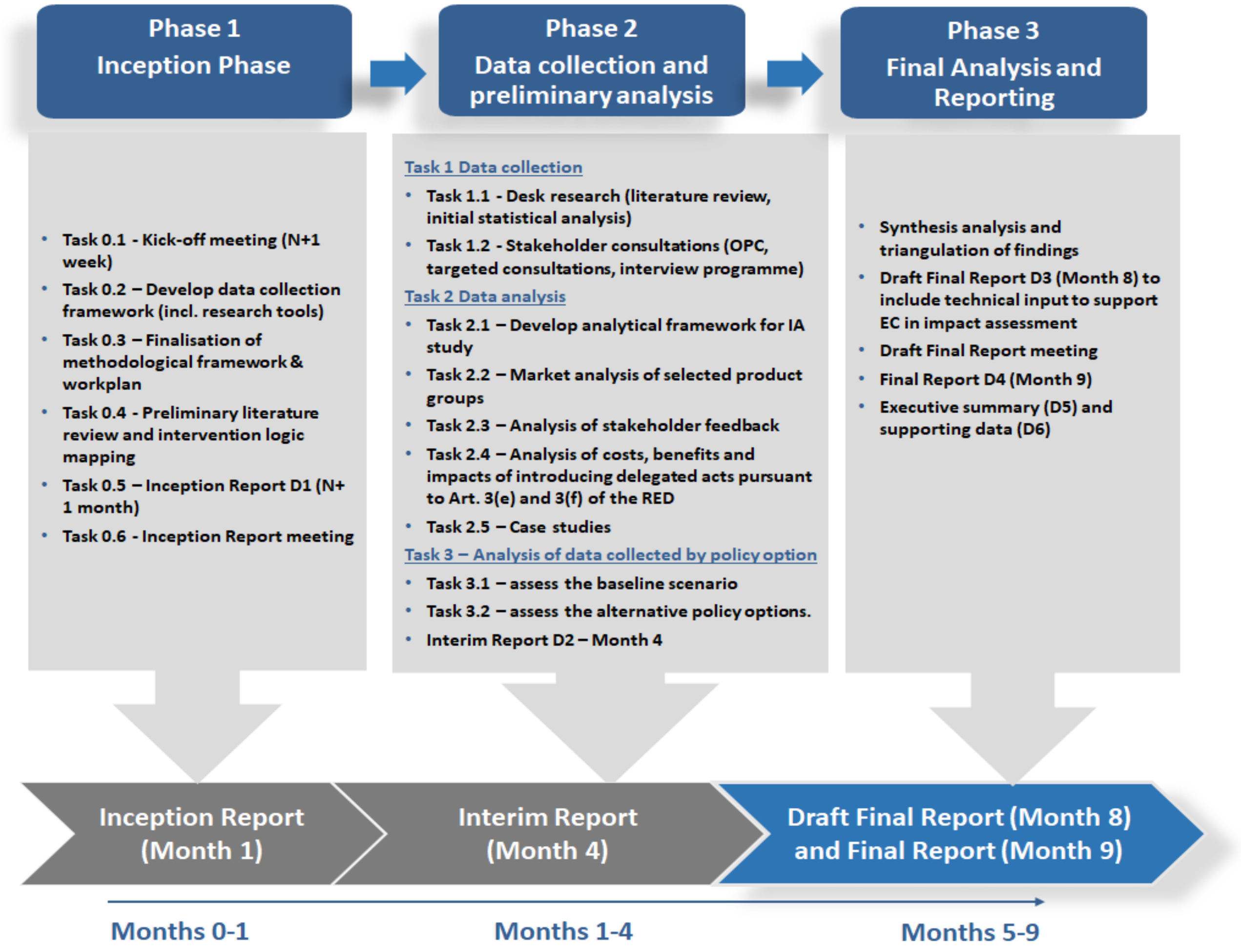
1.2.1 Methodological approach

The report is based on a combination of desk research, interviews and several online consultations. In addition, a series of case studies have been undertaken.

A short summary of the methodological approach being adopted is now provided. The assignment was undertaken in three phases, as set out in the following diagram:

[1] The legal basis for Delegated Acts is set out in Article 290.2 of the TFEU. They are defined as non-legislative acts of general application to supplement or amend certain non-essential elements of a legislative act, and define the objectives, content, scope and duration of the delegation.

Figure 1.1: Methodological approach



Phase 1
Inception Phase

- Task 0.1 - Kick-off meeting (N+1 week)
- Task 0.2 – Develop data collection framework (incl. research tools)
- Task 0.3 – Finalisation of methodological framework & workplan
- Task 0.4 - Preliminary literature review and intervention logic mapping
- Task 0.5 – Inception Report D1 (N+ 1 month)
- Task 0.6 - Inception Report meeting

Phase 2
Data collection and preliminary analysis

Task 1 Data collection

- Task 1.1 - Desk research (literature review, initial statistical analysis)
- Task 1.2 - Stakeholder consultations (OPC, targeted consultations, interview programme)

Task 2 Data analysis

- Task 2.1 – Develop analytical framework for IA study
- Task 2.2 – Market analysis of selected product groups
- Task 2.3 – Analysis of stakeholder feedback
- Task 2.4 – Analysis of costs, benefits and impacts of introducing delegated acts pursuant to Art. 3(e) and 3(f) of the RED
- Task 2.5 – Case studies

Task 3 – Analysis of data collected by policy option

- Task 3.1 – assess the baseline scenario
- Task 3.2 – assess the alternative policy options.
- Interim Report D2 – Month 4

Phase 3
Final Analysis and Reporting

- Synthesis analysis and triangulation of findings
- Draft Final Report D3 (Month 8) to include technical input to support EC in impact assessment
- Draft Final Report meeting
- Final Report D4 (Month 9)
- Executive summary (D5) and supporting data (D6)

Inception Report (Month 1)

Interim Report (Month 4)

Draft Final Report (Month 8) and Final Report (Month 9)

Months 0-1

Months 1-4

Months 5-9

1.2.2 Results of the stakeholder consultations

This impact assessment (IA) 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. This built on the inception impact assessment carried out by the Commission in January- March 2019.

As regards the **interview programme**, 76 interviews were completed with a wide range of relevant stakeholders, namely manufacturers, companies specialising in cybersecurity and industry associations representing the interests of manufacturers of internet-connected radio equipment, as well as national authorities, market surveillance authorities and consumer associations. In addition, CSES made three presentations during the course of the study, a presentation to 40+ people attending the Radio Equipment Expert Group (RE EG) meeting in June 2019, a further virtual presentation to the RED ADCO at which more than 40 market surveillance authorities were present and lastly, a presentation of the findings to the RE EG in December 2019.

Regarding the two online surveys, Annex 6 provides an analysis of the **targeted consultation** responses. 56 respondents were received 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.

In respect of the **Open Public Consultation (OPC),** Annex 7 provides an analysis of the responses. As the topics covered are quite specialist, the survey response was only 42. The results were analysed and are presented in a separate annex. The OPC was carried out using the Commission's EUSurvey tool. 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.

Overall, taking a combination of the interview programme, OPC and targeted consultations, some 174 stakeholders took part, with a further circa 30 stakeholders consulted as part of interactive presentations made by the study team (e.g. to the RE EG and the RED ADCO).

1.2.3 Analytical framework

The IA has been structured in a way that has allowed a number of key issues common to all IAs to be assessed. In particular, the following components collectively form the analytical framework underlying the study:

1. Analysis of the EU policy and legal context;
2. Analysis of the nature and extent of the problem;
3. Assessment of why the EU should consider taking action and as to what could be achieved through EU-level action compared with national action alone.
4. A review of the alternative policy options defined in the Tender Specifications to achieve policy objectives.
5. Assessment of the economic, social and environmental impacts of the different policy options, and of which stakeholders will be affected.
6. Analysis as to how the different options compare (efficiency, effectiveness and coherence) and identification of a preferred policy option.
7. Assessment of how monitoring and evaluation arrangements should be organised for the preferred policy option identified.

In the table below, the different steps involved in the IA process are outlined. These are then linked to the key study issues to be addressed. Examples of questions to investigate the costs, benefits and impacts are then provided.

Table 1.1: Steps in the Impact Assessment process

Steps in the IA process	Short overview & description
Identify the political and legal context	The political and legal context underlying the impact assessment was analysed. In particular, the regulatory framework was examined, including the RED's essential requirements, the provisions already included in the Directive for delegated acts, including the two within scope.
Step 1 – Define the problem	The problem definition required an analysis of the nature, scale and magnitude of the problem. The stakeholders which would be affected (directly and indirectly) were identified, the nature of the problem and its scale, the causes, consequences, and any unintended effects were assessed. The problem definition also identified and analysed EU policy-making needs.

Steps in the IA process	Short overview & description
Step 2 – Identify the rationale for EU intervention	The rationale for EU intervention was then assessed to determine the European added value in relation to each policy option. A key consideration was how far it could be possible to achieve similar objectives and outcomes without a regulatory approach (i.e. the activation of Art. 3(3)e and 3(3)f, for example by strengthening the effectiveness of existing EU legislation or through a self-regulation approach.
Step 3 – Identify and define the policy objectives	DG GROW's inception impact assessment defined the overall EU policy objective as being to ***"ensure an adequate level of security for internet-connected radio equipment and wearable RE at the moment of placing on the market".*** Further consideration of the policy objectives, and how these are linked with the wider EU policy and regulatory framework has been given. The policy options ("PO") defined were: • Option 0 - baseline scenario (no activation of the delegated acts) • Option 1 - industry self-regulation • Option 2 - adoption of a delegated act pursuant Article 3(3)(e), with safeguards to ensure protection of personal data and privacy • Option 3 - adoption of a delegated act pursuant Article 3(3)(f). Radio equipment would be required to incorporate certain features ensuring protection from fraud. • Option 4 - adoption of a delegated act pursuant both Articles 3(3)(e) and (f). • Option 5 - Horizontal regulation covering the cybersecurity of all industrial products (covering data protection and privacy and protection from fraud). [2]
Step 4 – Analyse and compare the policy options	The next step was to analyse comparatively the above PO on the basis of their expected economic, social and environmental impacts. The costs and benefits will need to be quantified whenever possible. We will clearly differentiate between monetised and non-monetised costs. A quantitative and qualitative comparative assessment of the PO will be supplemented by a graphical presentation of the advantages and disadvantages of the different PO using a scale to indicate how positive or negative the effects are likely to be. The regulatory policy-on options (2, 3 and 4) will be compared with the self-regulatory policy-off option (1) and with the counterfactual situation (0).
Step 5 – Identify the preferred policy option	Having reviewed and analysed the different PO in detail, a preferred PO will then be identified. This will be justified on the basis of a thorough assessment of the advantages and disadvantages of each PO outlined in Step 5. Whilst most PO are mutually exclusive due to the way in which these have been clearly defined, it may still be possible to combine a regulatory option, with some policy measures, such as awareness-raising about the risks, and promoting good practices among industry.
Step 6 – Determine monitoring and evaluation arrangements	Based on the preferred PO identified, put forward appropriate monitoring and evaluation arrangements. This will need to consider the importance of putting in place appropriate indicators and judgement criteria to assess the extent of the future initiative's successful implementation from the outset.

In order to carry out the above steps, an analytical framework was developed in the form of a key study issues framework. This was considered in the design of research tools (interview guides and online questionnaires) in Phase 1. The key study issues were developed by our team and are set out in Annex 2.

[2] It should be noted that this policy option was identified subsequently and was not included in the Tender Specifications or inception impact assessment, but was suggested bottom-up by stakeholders.

1.3 Definitions

This study focuses on particular aspects of the RED relating to ensuring strengthened safeguards for data protection and privacy and protection from fraud in connected radio equipment products and wearables. However, implementing these principles requires setting out common definitions so that there is a shared understanding of these concepts and what they might mean in an Internet of Things (IoT) context. The following terms are therefore defined upfront in Section 1.3:

- The Internet of Things;
- Personal data, data protection and privacy;
- Protection from fraud; and
- Data protection and privacy by design and default.

1.3.1 Definition of the Internet of Things

The internet has evolved in the past five years or so into the Internet of Things ("IoT"), a system of interrelated internet-connected devices, mechanical and digital machines[3], objects (embedded with sensors, software, and other technologies[4]) with the ability to transfer data over a network. As will be demonstrated in Section 2.2 (broader study context) and in Section 3.1.2 - market size and structure), the IoT 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.

Some academic literature points to there being many different definitions and interpretations of the IoT (see *inter alia,* Atzori, Iera, and Morabito 2010; Bandyopadhyay and Sen 2011; Malina et al. 2016). The IoT 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. The IoT will assist in the optimisation of processes through advanced data analytics, and be the catalyst for new market segments by capitalising on its cyber-physical characteristics, giving rise to cross-cutting applications and services (Miorandi et al. 2012)". [5]

However, it also raises a series of specific challenges in terms of the risks that could occur both in respect of device-level security, and the attendant implications for data protection and privacy and protection from fraud, but also the risk of network attacks such as through the use of BotNets with the risk of the manipulation of large numbers of connected but unprotected IoT devices with radio equipment functionality (i.e. falling within the RED's scope). Further details regarding the implications of the IoT in a data protection and privacy context are outlined in a review of key literature provided in Section 3.3.2 Data protection and privacy in the context of connected radio equipment and wearables.

1.3.2 Definition of personal data, data protection and privacy

In this sub-section, definitions of the terms personal data, data protection and privacy are considered. It should be noted that these consider both the legal definition provided under existing primary and secondary EU law, which delineates the boundary for the possible activation of the delegated acts under the RED, but also the broader, common understanding of these terms in wider literature.

Personal data is defined in Article 4(1) of the GDPR as any information relating to an identified or identifiable natural person,, either directly or indirectly. The European Commission's DG JUST

[3] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[4] https://www.oracle.com/internet-of-things/what-is-iot.html

[5] Security and privacy in the internet of things, Carsten Maple, 2017 - https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1366536?src=recsys

Questions and Answers indicates that personal data is data that has been *"de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR. However, personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible. The GDPR protects personal data regardless of the technology used for processing that data – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order)"*[6].

Regarding the **types of data that constitutes personal data**[7], this includes any information (whether held electronically or physically) relating to an identified or identifiable individual (i.e. not companies or other organisations). It includes for example information such as: Names, Addresses (including email addresses), Telephone / mobile numbers, Dates of birth, Job titles and any Online identifiers (e.g. IP addresses). The definition is actually much broader and encompasses any information that relates to an individual. There is a further 'special category' of 'sensitive personal data' which includes information about: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health and data concerning a natural person's sex life or sexual orientation.

Data protection and privacy are fundamental rights enshrined in EU primary and secondary law. The **right to data** protection is a fundamental right guaranteed in Article 8 of the Charter of Fundamental Rights of the EU (CFR). Article 8 of the Charter lays down a system of checks and balances to ensure full respect of the right to data protection, including the supervision of its effective application by an independent authority. **The right to privacy** is guaranteed in Article 7 of the Charter which provides that *'everyone has the right to respect for his or her private and family life, home and communications'*. Article 8 of the European Convention on Human Rights (ECHR) also provides for the right to privacy.

The reference in Art. 3(3)(e) of the RED to the possible activation of a delegated act in respect of data protection and privacy needs to take into account the legal definition of these issues in existing EU legislation, as this provides a reference point as to the legal limits of the delegated act foreseen in the RED. Art. 4 (1) – Art. 4(5) provide definitions of the GDPR relevant to this study as per the table below:

Table 1.2: Art. 4 Definitions of the GDPR points 1-5

Type of data	Article	Article text
'Personal data'	Article 4(1)	…means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
'Processing'	Article 4(2)	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

[6] The European Commission's DG JUST is responsible for the GDPR. It has issued a Questions and Answers on the GDPR here https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en. The legal definition of personal data is laid down in the legislation (see table on next page).

[7] See https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Type of data	Article	Article text
		transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
'Restriction of processing'	Article 4(3)	…means the marking of stored personal data with the aim of limiting their processing in the future;
'Profiling'	Article 4(4)	…means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
'Pseudonymisation'	Article 4(5)	…means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (e.g. identifiers8), provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
'Personal data breach'	Article 4(12)	….means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

The GDPR applies to the collection and processing of personal data by data controllers and data processors providing services (and indirectly, implicitly impacts manufacturers and technology providers). It is interesting to note that in a connected radio equipment and wearables context, data breaches may result from a device-level breach, a local network breach e.g. a home network with multiple connected IoT devices or a breach during the transmission of data being collected from connected RE devices being collected by the data processor. Therefore, data protection and privacy issues primarily relate to the processing of personal data under the responsibility of the data controllers and, where applicable of data processors, and indirectly concern whichever other economic operators (EO) are involved in the value chain (e.g. manufacturers, technology providers).

According to the guidelines published by the European Data Protection Board (EDPB) on personal data breach notification under the GDPR, [9]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.

It is also important to understand **what consent means** in the sense of connected RE products and devices and the data they collect. This is especially pertinent for consumer IoT products, which may collect personal data about an individual, and about how those individuals use a particular product.

Under the GDPR, which came into effect on 25th May 2018, consent 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)). The conditions for consent are further established in Article 7. It is worth noting

[8] There are different technologies that could identify individuals. An example is Radio Frequency Identification (RFID) tags, whose usage is somewhat controversial, given the potential to identify people by their geolocation.

[9] Guidance available from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

that the definition of consent under the GDPR also applies for purpose of obtaining consent under the ePrivacy Directive 2002/58/EC, in particular as concerns the placing of cookies and other online trackers.

A further important Article in the GDPR of relevance to this study is **Article 5 - Principles relating to the processing of personal data.** This concerns how personal data should be collected, and addresses key issues relating to data processing. Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b. 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');

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') ; (…).

Personal data shall also be accurate and kept up to date ('accuracy', Art. 5(d)); kept for no longer than is necessary ('storage limitation', Art.5(e)); and processed in a manner that ensures appropriate security of the personal data ('integrity and confidentiality', Art. 5(f)).

Article 6 builds on the above by detailing the six legal bases for lawful processing of personal data. These include: i) that the data subject has consented; ii) that the collection and processing is necessary for the performance of a contract; iii) that the controller processes the personal data pursuant to a legal obligation; iv) that the processing is in the vital interests of the data subject; v) that the processing is necessary to conduct a task that is in the public interest; or vi) that the data are processed for the purposes of a legitimate interest pursued by the data controller (Article 6(1)(a-f)).

Chapter III of the GDPR lays down in more details the rights of individuals in respect of their personal data, which includes the right to transparent information, the rights to have access to one's personal data and to have the data rectified, erased, restricted or ported, as well as the rights to object and not to be subject to automated individual decision-making.

1.3.3 Definition of data protection by design and default

Data protection by design and default principles have been integrated into the GDPR's requirements in Article 25. These require data controllers to put in place appropriate technical and organisational measures (Art. 24) to implement data protection principles and to safeguard individuals' rights. In practice, this means implementing data protection principles into data processing activities and business practices, from design stage throughout the data collection lifecycle.

This concept builds on the 'privacy by design' concepts, which was developed under previous data protection laws. However, the GDPR has made data protection and privacy by design and default a legal requirement. Integrating data protection by design and default is about considering data protection and privacy issues upfront in everything that data controllers and processors do so as to comply with the GDPR's principles and requirements[10].

The GDPR's risk-based approach focuses on the concept of data controllers and processors demonstrating accountability, so as to show how they are complying with the requirements. An example of a checklist relating to how a data controller or processor might comply with data

[10] Draft EDPB guidance on data protection by design was published in 2019: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_env

protection by design and default principles[11] is provided in Annex 4. In the analysis of existing EU legislation (Section 3.3), issues around the GDPR and what its implementation means in terms of the collection of personal data for connected RE products is considered, including how far this affords consumers and businesses using RE products sufficient protection.

1.3.4 Definition of protection from fraud

Unlike data protection by design and default, where a definition is provided in the GDPR of key relevant terms[12], "protection from fraud" is not presently defined in any EU legislation. Whilst the Non-Cash Payments Directive (Directive (EU) 2019/713) does not define fraud and the counterfeiting of non-cash means of payment, a harmonised definition should cover new types of non-cash payment instruments that allow for the transfer of electronic money and virtual currencies.

To the extent that a definition exists in international law, fraud involves intentional deception to secure unfair or unlawful gain, or to deprive a victim of a legal right. In some jurisdictions such as the U.S., a distinction is made between criminal and civil fraud.

In the absence of a suitable legal definition at EU level, it is also necessary to consider how fraud has been defined in dictionaries. Examples are the *"Intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right"*[13] and an *"act of deceiving or misrepresenting"*.

In the RED, there is a reference in Art. 3(3)(f) to *"safeguards to ensure protection from fraud"* but this is without a definition. There are many different types of fraud, such as credit card fraud, the falsification of documents or information on user credentials, and fraud by false representation. Whereas fraud is often understood in a financial sense, in a connected RE and wearables context, it may involve either financial fraud (e.g. debit and credit card fraud), or data theft or other types of crimes such as the theft of personal data and information, extending to identify theft (including misrepresenting someone by appropriating their user credentials).

Several pieces of literature on fraud in the context of the IoT[14] were identified, although this is a nascent area. For instance, a blog on the evolution of fraud notes the increasing sophistication of IoT fraud. *"At a basic level, it's easy to understand this fraud. Connected devices that provide increased convenience and improved services are also collecting, transmitting and storing vast amounts of consumer data, and creating a number of new theft and privacy risks. As a result, with everything connected to Internet theoretically able to be hacked, millions of new devices, business processes and network connections have now become hackable".*

A further risk in respect of IoT devices is that financial data is often stored by consumers on smartwatches, phones and other connected devices. As many IoT devices are consumer IoT focused (and such devices are more likely to lack basic security functionality), they may contain data and information that is highly personal and sensitive. Such devices are not always secured properly or used on private connections.

Some of the vulnerabilities in IoT products and devices also pose risks relating to the use of large numbers of devices that can be used to launch botnet attacks. An example of a type of fraud that is very prevalent across many IoT devices is ad fraud, as per the following example. This shows the link

[11] Explanation of the concepts of data protection and privacy by design and default, European Commission, DG Justice, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en

[12] Examples of definitions provided in the GDPR are: data protection, data breaches, data protection by design and by default and consent

[13] https://www.merriam-webster.com/dictionary/fraud

[14] https://www.syniverse.com/blog/connectivity/understanding-emerging-fraud-internet-things/

between Art. 3(3)d, 3(3)(e) and 3(3)(f). Moreover, it also shows the multi-dimensional nature of potential frauds and commonalities across many different types of connected RE products/ devices.

Attacks may 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. This botnet risk perpetrated through ad fraud underlies a central threat of IoT fraud: It's not the devices themselves that present the security risk as much as the Trojan horses they represent in terms of security vulnerabilities.

Many newer IoT devices, such as baby monitors and refrigerators, don't even have security systems protecting them from botnet attacks because of their limited memory and slow processors. 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. Ad fraud offers one of the biggest third-party codes available to exploit users' devices and is much easier than a brute-force attack. As a result, the botnet risk is a serious one, and one for which protection against cannot be guaranteed because of ad fraud vulnerabilities, among other factors.

Source: https://www.syniverse.com/blog/connectivity/understanding-emerging-fraud-internet-things/

1.3.5 Definition of security by design and default

Whereas this study focuses on data protection and privacy and protection from fraud in the context of the RED, it is important to stress the importance of a holistic approach to RE product and device security, as minimum security requirements at connected RE product and device level are essential as a pre-requisite for preventing data breaches, which could in turn lead to data loss, which may lead to data protection and privacy being undermined, and compromise personal data and result in increased risk of fraud. Therefore, the **concept of security by design and default** is of relevance, as if products are designed in a secure way from the outset, they are less likely to lead to personal data breaches, result in privacy being compromised or on a connected RE device user becoming a victim of fraud.

Security by design and default can be defined as taking a holistic approach to ensuring that security is built into the design and manufacturing process from the outset so that any potential security vulnerabilities are thought through in advance. These may relate to the operating system, hardware and software. Of course, this cannot eliminate all possible security vulnerabilities, especially for software where new threats and vulnerabilities may emerge subsequently. However, adhering to these principles from the outset could help to ensure that producers design connected RE products and wearables in a way that ensures basic security functionality and thereby eliminates reduces the risk of device penetration and data breaches (which in turn could lead to data loss, personal data protection and privacy being compromised, and a risk of fraud being perpetrated.

An overarching explanation of relevant issues in this regard is provided by Section 3.2 - Conceptualisation of radio equipment security risks, consequences and solutions. This study has built on stakeholder feedback received in response to the publication of an **inception impact assessment**[15] **managed by the European Commission's DG GROW**, which required an online consultation undertaken with industry associations, consumer associations and wider stakeholders held in January – March 2019. It will also take into account the results of two online consultations carried out between August and mid-November 2019, the first an Open Public Consultation (OPC) and the second a targeted consultation.

Through the impact assessment study, the **costs, benefits and impacts** of going ahead with different alternative policy options are being investigated. The study will examine the impact on stakeholders

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

that would be affected by possible future regulations (or voluntary codes of conduct), such as economic operators (especially manufacturers, but also distributors and importers), national authorities and market surveillance authorities ("MSAs").

This study will assess **the impacts of either regulating or adopting a non-regulatory approach** to addressing risks linked to data protection and privacy, and to protection from fraud pertaining to internet-connected radio equipment and wearables. Accordingly, the study will **assess the security vulnerabilities**, and the extent to which there are any similarities and differences in the nature across different product classes, taking into account the probability of such vulnerabilities being exploited through a risk assessment to identify similarities and differences across different types of connected radio equipment and wearables. Such risks may vary, for example, depending on a number of factors, such as how different types of radio equipment and wearables are connected to the internet, whether *directly* through a wireless network or router, or *indirectly*, through a Bluetooth connection or via a link between an IoT device and a mobile phone application.

1.4 Structure of the final report

The report is structured as follows:

- **Section 1 – Introduction.** Sets out the study objectives and scope, and outlines definitions relevant to the study supporting the Impact Assessment. Provides a summary of the methodology and an overall analytical framework, and outlines a set of key study issues for the IA in supporting annex;
- **Section 2 – Background and policy context.** Examines the EU policy and regulatory context relevant to issues relating to data protection and privacy and protection from fraud in an IoT context;
- **Section 3 – Problem Definition.** Key trends in respect of the growth of connected radio equipment and wearables (especially consumer IoT devices and products) are examined. The extent to which security vulnerabilities in connected RE products can be identified across different classes of connected RE is analysed. The current EU regulatory framework, and extent to which there are any gaps, overlaps and inconsistencies between the RED, proposed DAs and other relevant EU legislation are analysed;
- **Section 4 - Assessment of risks, vulnerabilities and consequences of breaches.** Considers the findings from the mapping of risks, security vulnerabilities and possible technical solutions.
- **Section 5 - Review of Policy Options, Cost-benefit Assessment and review of Impacts.** Sets out the policy options at EU level under consideration through the IA, and considers the costs and benefits, as well as the economic, social and other impacts associated with these different options. Based on the impact assessment, a preferred policy option is identified;
- **Section 6 – Key findings and conclusions.** Outlines the main findings from the IA and considers the way forward including the identification of a preferred policy option and of alternative viable options.

The main report structure (Sections 3 to 5) follows the broad structure set out in the Commission guidelines for an impact assessment. The analysis presented in Sections 3-5 draws on the findings from the desk research and analysis of stakeholder feedback based on a combination of interview feedback and feedback received through the targeted and OPC stakeholder consultations. The report is supported by supporting annexes:

- A bibliography (Annex 1);
- Key study issues (Annex 2)
- List of interviews completed and scheduled (Annex 3);

- Analysis of the Consultation Responses received to the Inception Impact Assessment (Annex 4);
- Checklist data protection and privacy by design and by default (Annex 5)
- Product data on market size and structure, including forecasts (Annex 6);
- Analysis of responses to the OPC consultation (Annex 7); and
- Analysis of responses to the targeted consultation (Annex 8).

The analysis of responses to the OPC consultation (Annex 7); and the Analysis of responses to the targeted consultation (Annex 8) have been produced as separate standalone annexes.

2. Background and policy context

The background to the impact assessment study is examined, and the overall EU policy and legal context is now considered. The broad context is also provided regarding concerns in respect of data protection and privacy and protection from fraud in the context of connected radio equipment and wearables.

2.1 Background and policy context

2.1.1 Legal framework – an overview of the Radio Equipment Directive

The Radio Equipment Directive ("RED") establishes a **regulatory framework for placing radio equipment ("RE") on the Single Market**. Article 3(1) and Article 3(2) of the RED set out the **essential requirements** that RE shall respect, relating to health and safety, electromagnetic compatibility and radio spectrum. In particular:

> Article 3(1) *"Radio equipment shall be constructed so as to ensure: (a) the protection of health and safety of persons and of domestic animals and the protection of property, including the objectives with respect to safety requirements set out in Directive 2014/35/EU, but with no voltage limit applying; (b) an adequate level of electromagnetic compatibility as set out in Directive 2014/30/EU".*
>
> Article 3(2) *"Radio equipment shall be so constructed that it both effectively uses and supports the efficient use of radio spectrum in order to avoid harmful interference".*

Article 3(3) provides the basis for further delegated regulation governing additional aspects, empowering the Commission to adopt delegated acts and to specify which categories or classes of RE are concerned by each of the requirements set out in its points (a) to (i). The requirements referred to in points (a) to (i) relate to interoperability, emergency services, software, fraud, accessibility, privacy, personal data and misuse. This particular impact assessment pertains to Articles 3(3)(e) and 3(3)(f), i.e. data protection and privacy and protection from fraud respectively.

In common with other industrial product legislation implemented under the New Legislative Framework ("NLF"), the Directive is based on Article 114 of the TFEU (the approximation of laws)[16]. The RED's scope covers devices that use the radio spectrum for communication and/or radio determination purposes. All internet-connected radio equipment, including wireless consumer Internet of Things ("IoT") devices and wearables fall under the Directive's scope.

The two sub-articles within the scope of this impact assessment are **Article 3(3)(e), to ensure safeguards for the protection of personal data and privacy** and **Article 3(3)(f), contributing towards protection from fraud**. In the following table, the complete list of delegated acts that could potentially be activated is indicated, with the two in study scope highlighted in bold.

Table 2.1: Delegated Acts possible under Article 3(3e) and 3(3f)

3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:
a. radio equipment interworks with accessories, in particular with common chargers;

[16] 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".

b. radio equipment interworks via networks with other radio equipment;

c. radio equipment can be connected to interfaces of the appropriate type throughout the Union;

d. radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;

e. radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;

f. radio equipment supports certain features ensuring protection from fraud;

g. radio equipment supports certain features ensuring access to emergency services;

h. radio equipment supports certain features in order to facilitate its use by users with a disability;

i. radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated. The Commission shall be empowered to adopt delegated acts in accordance with Article 44 specifying which categories or classes of radio equipment are concerned by each of the requirements set out in points (a) to (i) of the first subparagraph of this paragraph.

Whereas the essential requirements have traditionally focused on (physical) product safety, some stakeholders have pointed to the need for greater recognition of the **linkages between product security (especially security) and safety**. This includes concerns relating to ensuring that there are **adequate levels of data protection and privacy in consumer IoT products** and other **smart devices.** Concerns in these areas have become more widespread across many areas of economic activity and society. The General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 came into effect in May 2018 and addresses many different data protection and privacy issues.

The current EU regulatory framework, extending beyond the RED itself to other key legislation, such as the GDPR (including Article 25 on data protection by design and default) are examined as part of the problem definition (Section 3).

2.1.2 Broader study context

The context to the study is the rapid growth in **internet-connected products (including IoT devices) that embed radio functionality.** In parallel, there are growing concerns as to whether **connected radio equipment, such as (but not limited to) IoT devices are sufficiently secure to be able to protect consumers and professional users in ensuring that their personal data is protected and privacy respected.**

Alongside the proliferation of connected radio equipment (“RE”) devices, cyber-attacks are, on one level, getting easier to implement (i.e. hackers can conduct one with limited technical expertise), and, at a different level, some forms of cyberattacks are becoming more sophisticated, complex and monetised. These considerations are introduced in this section, and then examined in greater detail under Section 3 (problem definition).

The growth in internet-connected RE devices – especially consumer IoT devices - is a trend likely to increase even further in future. There has been a major trend in parallel towards **smarter and more complex products being put on the market,** which are connected either directly or indirectly to the internet. Products newly integrating connectivity capabilities such as many household appliances (e.g. ovens, fridges, washing machines) would traditionally not have been subject to the RED, but due to the integration of radio devices within many electrical appliances and other smart devices, now fall within its scope. Since there are ever-more ‘smart’ devices in consumers’ homes, such as smart TVs, internet-connected toys, smart meters, and connected washing machines, ovens, toasters, CCTV and other types of monitors, etc. the importance of ensuring that the security of such consumer products is strengthened has increased.

In terms of market size, according to a market research report by Gartner, **connected devices are *"expected to boom to 20.4 billion units by 2020"***[17], which means that the number of IoT devices will significantly exceed the world's population. Of these, devices, consumer IoT devices account for approximately 63% of the projected total:

Table 2.2: IoT Units installed base by category (millions of units)

Category	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	6,381.8	8,380.6	11,196.6	20,415.4

Whilst recognising the **considerable economic, social and environmental potential of the IoT**, at the same time, the IoT "poses significant privacy, security, and data protection challenges and it has demanded a closer look into how the EU legal framework is applied in the IoT context"[18]. Moreover, the same academic thesis points out that "as the traditional Internet has developed into the IoT, personal data protection law has also expanded from being a niche field of law, into a legal area that is applicable in almost all sectors, services, and technologies. Globalisation and the vast technological development, and elaborated collection of data, has raised questions about whether the current EU data protection legislation can cope with the new challenges that the IoT poses"[19]. Further issues relating to the application of the legal framework – especially the GDPR, the e-Privacy Directive and the proposed ePrivacy Regulation - is sufficiently fit for purpose in an IoT context are examined in Section 3.3.2 - Data protection and privacy in the context of connected radio equipment and wearables.

The European Commission's inception impact assessment published January 28th 2019[20] pointed out that whilst RE is used on a daily basis by consumers and professional users, vulnerable users, such as children and the elderly are also among the user groups where security vulnerabilities may pose greater risks, due to their lack of awareness of cybersecurity. They may therefore be at greater risk regarding data protection and privacy breaches and exposure to fraud. Although the GDPR highlights in Recital 38 GDPR, that "children merit specific protection with regard to their personal data", research by the Norwegian Consumer Council has reported that there is a lack of adequate protection of children's rights to privacy and security in internet-connected toys available on the market.

> *"Internet-connected toys are "smart" and can interpret speech, making 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, according to the integrated sensors. To enable these new features, these products are equipped with speakers, and microphones and other sensors, and they can be connected to phones/tablets or directly to the internet. The ability of these products to record, store and share information raises concerns about safety, security, privacy and social development"*[21].

[17] Tung, L. (2017). IoT devices will outnumber the world's population this year for the first time. *Zdnet*, February 7, 2017. https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/ The article references a report by Gartner outlining projections in consumer IoT devices to 2020.

[18] PERSONAL DATA PROTECTION ON THE INTERNET OF THINGS - AN EU PERSPECTIVE, Jenna Lindqvist (2018) - Faculty of Law, University of Helsinki, Finland

[19] Idem.

[20] European Commission. Internet-connected radio equipment and wearable radio equipment https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-6426936_en

[21] Background paper on European Commission's Inception impact assessment on Internet-connected radio equipment and wearable radio equipment, page 1. Available from: https://ec.europa.eu/info/law/better-regulation/initiative/2018/publication/380959/attachment/090166e5c0fe9eed_en

The background paper to the inception IA states that in order to address risks, it would potentially be beneficial to apply at least a **minimum level of baseline security requirements** (as regards data protection and privacy and protection from fraud by design) to all RE, irrespective as to whether such RE is directly or indirectly connected to the internet. The inception IA also notes that *"IoT development brings the need for improved digital security not only for individual users but also for society as a whole"*.

There has also been exponential growth in **connected wearable products** on the market, such as smart watches and fitness products. Applications developed for smart wearable devices have certain vulnerabilities that may allow a third party to use an app to keep in touch with, and/or to track the location of users, which raises privacy concerns, given the risks associated with third parties accessing geolocalisation data. A specific example is smartwatches aimed at children. However, striking a balance is key, as many parents use geolocalisation data to keep track of their children's whereabouts.

> *"These devices may also contain a SIM-card, allowing children to connect to the Internet through mobile-networks or a Wi-Fi connection. In its most basic form, the smartwatch functions as a mobile phone or a tablet attached to the wrist, which connects to the parents' phones through an app. The use of a combination of GNSS and Internet data can also allow real-time location tracking and direct communication. In the same way, some smart wearable devices allow to use an application to keep in touch with and/or track the location of the users"*[22].

A review of available secondary research relevant to the issues covered by this study is presented in further detail in Section 3.1 (problem definition).

As noted above, cyber-attacks are becoming more common, both unsophisticated cyberattacks that are relatively straight forward to launch on the one hand, but also more sophisticated cyberattacks on the other. Moreover, obfuscation practices that help hackers and cyber-attackers to avoid detection have also become more common such that it may be difficult to detect when a consumer IoT device has been penetrated. Consequently, individual users of connected radio equipment and wearables may not even be aware that their personal data has been compromised or that they are at risk of fraud, or have already been defrauded until it is too late. The way in which device and home level data breaches can occur is analysed in the Section dealing with the conceptualisation of IoT security risks.

[22] Idem.

3. Problem definition

This section contains the problem definition. It provides an assessment of the baseline situation, including the nature and extent of the problem, and the identification of policy needs. The section includes:

- An assessment of the main trends and developments relating to connected radio equipment ("RE") products and wearables, including demand-side forecasts by category of such products;
- The identification and analysis of threats, vulnerabilities and the impacts associated with inadequate security in RE products and wearables, differentiating between different types of products e.g. simple and complex products;
- Consideration of the consequences of data protection and privacy breaches and fraud and consideration of the nature and magnitude of the risks if potential threats and vulnerabilities are not designed-out or mitigated from the outset.;
- Consideration as to whether there are specific types of consumers that are at particular risk, and whether a risk-based approach should be considered to address issues around the location where a connected RE device or wearable is expected to be used;
- A review of market size and structure by relevant NACE code type;
- A review of the existing EU regulatory framework and an analysis of regulatory gaps, considering the RED and wider EU legislation; and
- A review of relevant regulatory and non-regulatory developments nationally and internationally relevant to strengthening data protection and privacy and protection from fraud in connected RE devices and wearables, such as by improving the integration of basic security functionality in consumer IoT devices and products through the adoption of minimum baseline security requirements.

3.1 Key trends and review of market size and structure for connected radio equipment

This section contains:

- A review of key trends in RE products;
- A demand-side summary of projected demand for different types of connected RE products; and
- A review of the characteristics of the RE market, in terms of market size and structure.

3.1.1 Trends in radio equipment products

As noted in the background section (see Section 2.1.2 – broader study context), there has been a significant increase in the volume of connected RE products and wearables placed on the European Single Market in the past 10 years, reflecting the growth in the ubiquity of Internet of Things (IoT) devices. In this section, different categories of RE are presented. Demand-side forecasts for these devices are then outlined, followed by an overview of market size and structure in respect of producers of connected RE.

3.1.1.1 Categories of radio equipment

This section provides an overview of the application categories for connected RE. These were first developed by the European Commission as part of research undertaken by Tech4i2 published in

2016[23]. Annex 4 (see separate standalone annex) provides more comprehensive insights into market size and structure across more than 30 different types of devices that comprise the application categories.

Radio equipment application categories

Research undertaken in 2015 categorised licence exempt radio equipment[24] into seven application categories (medical devices are excluded from the scope of the present study). Categorisation was achieved by grouping radio equipment into the licence exempt spectrum groups, as shown in the following table. Most of the application categories were drawn from EC Decision 2013/752/EU[25], and additional applications and devices have been identified from other decisions or EC recommendations.

Table 3.1: Categorisation of radio equipment

Application categories	Device type
Radio-frequency identification (RFID)	Handheld, fixed payment, fixed tracker interrogators
Transport and traffic telematics	Embedded vehicle anti-collision radar, electronic fee collection, ITS, mobile data terminals on board vehicles
Smart home devices (alarms, telecommand and telemetry)	Wireless alarms, key fobs, baby monitors, garage door/gate openers, telemetry equipment, telecommand devices
Audio/media wireless streaming	Mini FM transmitters, cordless headphones, media players, speakers, wireless microphones
Remote monitoring and wireless alarms	Utility meters, social alarms, distress alarms
Wideband data transmission	Tablets, smartphones, games consoles, media players, speakers, smart TVs, connected car, wearable devices, toys and drones

Source: 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.

The categorisation of products is important because it provides the basis for the study to examine more closely the diverse types of vulnerabilities and security breaches for different application categories that may potentially risk compromising data protection and privacy and which could lead to exposure to fraud. It also enables the number of devices susceptible to these vulnerabilities to be understood.

3.1.1.2 Radio equipment market forecasts

Decisions concerning the Radio Equipment Directive 2014/53/EU, particularly Article 3(3)(e) and (f), need to have robust understanding of the size of the market for radio equipment in EU28 Member States and the number of devices in different application categories now and in the future. Therefore, this section provides a brief introduction to the utilisation of different types of radio devices between

[23] 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

[24] Licenced equipment primarily concerns device utilising spectrum (for 2g, 3g, 4g and 5g) purchased by mobile telecommunications operators. The main item of equipment is currently mobile telephony handsets. These make up a very small proportion of the total market of nearly one billion radio equipment devices forecast for 2020.

[25] 2013/752/EU: Commission Implementing Decision of 11 December 2013 amending Decision 2006/771/EC on harmonisation of the radio spectrum for use by short-range devices.

2015 and 2030. The evidence base for forecasts and further details about market trends for more than 30 radio devices can be found in Annex 4.

3.1.1.3 An overview of Radio Equipment forecasts

In the previously mentioned EC study[26] radio equipment utilisation between 2015 and 2030 was forecast for six[27] application categories and more than 30 types of devices.

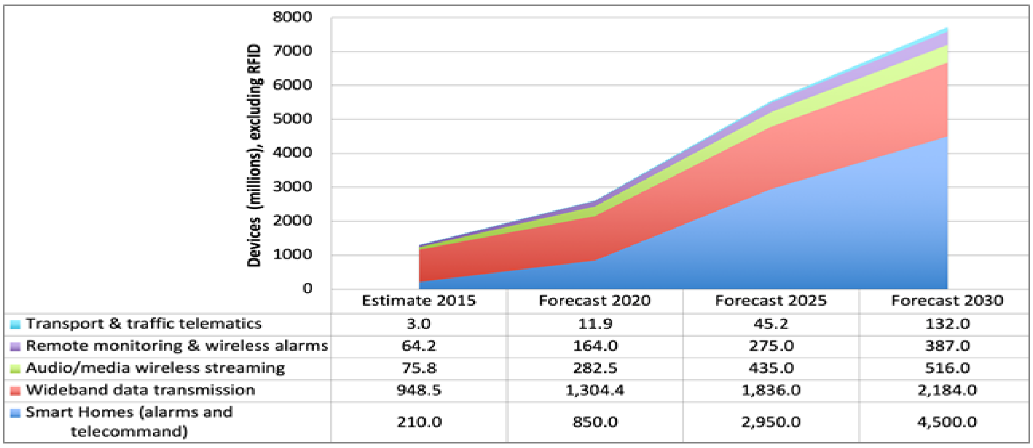
This study has revisited the 2016 study and, through desk research and interviews with experts, forecasts and predictions have been updated. This has led to small changes in previous forecasts. These mainly concern small changes and a reduction in the forecast for the number of tablets, since forecasters now expect sales to decrease in the future.

Figure 3.1 provides an overview of forecasts for the number of radio equipment devices that will be in use across the seven application categories between 2015 and 2030 in EU28 Member States. The figure omits RFID devices since they are inert and cannot transmit data[28].

Estimates suggest there were 1,097 million radio equipment devices in EU28 Member States in 2015. [29]This is estimated to rise to 7.43 billion by 2030. This represents a cumulative annual growth rate (CAGR) of 14.6 per cent. The largest application categories are expected to be devices associated with smart homes, there are expected to be 4.5 billion of these devices in use in EU28 Member States in 2030. 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 Wi-Fi and Bluetooth. There are expected to be 2.18 billion of these radio devices in use in EU28 Member States in 2030.

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 Wi-Fi and Bluetooth. There are expected to be 1.897 billion radio devices in use in EU28 Member States in 2030.

Figure 3.1: 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

[26] 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

[27] There were actually seven categories, but medical devices are outside the study scope, since they are covered separately in the Medical Devices Regulation (Regulation (EU) 2017/746).

[28] 99 per cent of RFID devices are 'passive'. They do not have an internal power source (e.g. battery) and cannot transmit data unless energy is provided from a nearby RFID reader's interrogating radio waves. Estimates suggest 3.7 billion RFID devices in 2015 and 58.8 billion are forecast in 2030.

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

Conclusion

These forecasts highlight the large number of radio equipment devices – 7.7 billion – that are forecast to be in use in EU28 Member States in 2030. This equates to 29 radio devices in each EU28 household in 2030[30].

The large number of RE devices and wearables sold into the European single market emphasises the significance of any decisions that might be made concerning the potential activation of Article 3(3)(e) and Article 3(3)(f) of the RED, or of alternative approaches to safeguarding data protection and privacy and protection from fraud.

The data estimates provided by Tech4i2 are among the best available. However, it is worth noting that it is difficult to predict growth in that "there are not even consistent figures for the number of devices connected to the internet today. Not only is there a significant difference in figures using the same definitions, but the issue concerning the varying interpretations of the IoT also has an impact. Some figures clearly state the difference between machine-to-machine (M2M) and IoT devices, such as those of the GSMA, whose analysis of M2M 'focuses on cellular M2M connectivity and excludes computing devices in consumer electronics such as smartphones, e- readers, tablets, as well as other types of M2M connection technologies that support the wider universe of the Internet of Things (IoT)" (Kechiche 2015).

3.1.2 Market size and structure

The preceding sections about radio equipment devices and wearables highlights the diversity of the different sub-sectors and product groups falling within the RED's scope. The research undertaken has identified the key NACE Rev 2 Groups (26 and 27[31]) and examined in detail the 34 descriptions of classes or sub-sectors. This analysis is presented in Annex 4. The research identified seven key NACE code classes that produce radio equipment (see Table 3.2) and five classes that produce the main components for RE (see Table 3.3 below). However, it should be noted that even within these seemingly tightly drawn sectoral definitions there could still be variance in the extent to which radio equipment and components are covered in the particular NACE class.

Table 3.2: The main NACE classes that produce radio equipment

NACE Class	Sector	Relevance
26.30	Manufacture of communication equipment	✓✓
26.40	Manufacture of consumer electronics	✓✓
27.51	Manufacture of electric domestic appliances	✓✓
27.90	Manufacture of other electrical equipment	✓✓
26.20	Manufacture of computers and peripheral equipment	✓
26.51	Manufacture of instruments and appliances for measuring, testing and navigation	✓
26.52	Manufacture of watches and clocks	✓✓

It was noticeable when considering relevant classes that some had slightly greater relevance to connected RE and wearables than others. These are indicated by a double tick in Table 3.2 above.

[30] Clearly devices will also be located in business 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 lfst_hhnhwhtc) is an overestimate, but it does serve to emphasis the enormous number of radio devices that are forecast in 2030.

[31] Eurostat NACE Rev.2 Statistical classification of economic activities in the European Community. https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF.

Table 3.3: The main NACE classes that produce components for radio equipment

Group Class	Title
26.11	Manufacture of electronic components and boards
26.12	Manufacture of electronic components
27.20	Manufacture of batteries and accumulators
27.32	Manufacture of other electronic and electric wires and cables
27.33	Manufacture of wiring devices

After identifying key sectors producing radio equipment and components, the characteristics of the sector were found in Eurostat's Structural Business Statistics (SBS) .[32] The radio device production classes are comprised of 39,217 enterprises, employing just over a million people (1,057,434), see Table 3.4. The table consists of the most recently available Eurostat data, although this predominantly relates to 2016 (different dates for some data are noted in the table). Across the different classes, radio equipment producers produced €296 billion of goods with an added value to production ratio of 24 per cent.

Table 3.4: Statistics for the main radio device NACE groups and classes 2016

NACE Class	Total Enterprises	Total Production Value (€m)	Value added at factors costs (€m)	Persons Employed
26.20 Computers & peripheral equipment	5,686	96,537	6,000 [A]	77,781
26.30 Communication equipment	6,000 [C]	33,346 [C]	9,903	142,785
26.40 Consumer electronics	2,831 [C]	20,847 [C]	3,274	54,065 [C]
26.51 Instruments & appliances	11,000	78,407	31,481	398,193
26.52 Watches & clocks	800	1,154	488	9,240
27.51 Electric domestic apps	2,000	35,237	10,167	172,370
27.90 Other electrical equipment	10,900 [C]	30,829 [C]	10,843	203,000 [C]
Total	39,217	296,357	72,156	1,057,434

[A] = 2014, [B] = 2015, [C] = 2017

Source: Eurostat SBS. Note – the data excludes Cyprus

The classes producing components used by radio devices are smaller in terms of enterprises – 14,466; 37 per cent the size of the radio device producers, see Table 3.5. But the component supplying classes are larger in terms of employment – 1.541 million employees; 45 per cent larger than the radio device producers. The data indicates that the average employment size of radio equipment producers (27 employees) is smaller than components suppliers (106 employees). It should obviously be highlighted that the items produced by components providers could be used in many other types of electronic equipment (e.g. not just radio equipment). It is difficult from Eurostat SBS data to obtain disaggregated product data only relating to connected RE products.

[32] Annual detailed enterprise statistics for industry (NACE Rev. 2, B-E) (sbs_na_ind_r2). https://ec.europa.eu/eurostat/web/structural-business-statistics/data/database.

The component producers produced €118 billion of goods. Radio equipment component producers had added value to the production ratio of 31 per cent, which is marginally greater than the ratio for radio equipment producers.

Table 3.5: Statistics for key components for radio device NACE groups and classes 2016

NACE Class	Total Enterprises	Total Production Value (€m)	Value added at factors costs (€m)	Persons Employed
26.11 Electronic components	7,000	51,240	20,068	214,655
26.12 Electronic boards	3,089	13,695	3,946	75,335
27.20 Batteries & accumulators	500 ^{C}	9,592	n/a	31,250 ^{C}
27.32 Other electric wires & cables	2,028	25,986	5,146	103,252
27.33 Wiring devices	1,849	17,795	7,728	111,6733
Total	14,466	118,308	36,888	1,541,225

^{C} = 2017, n/a not available

Source: Eurostat SBS

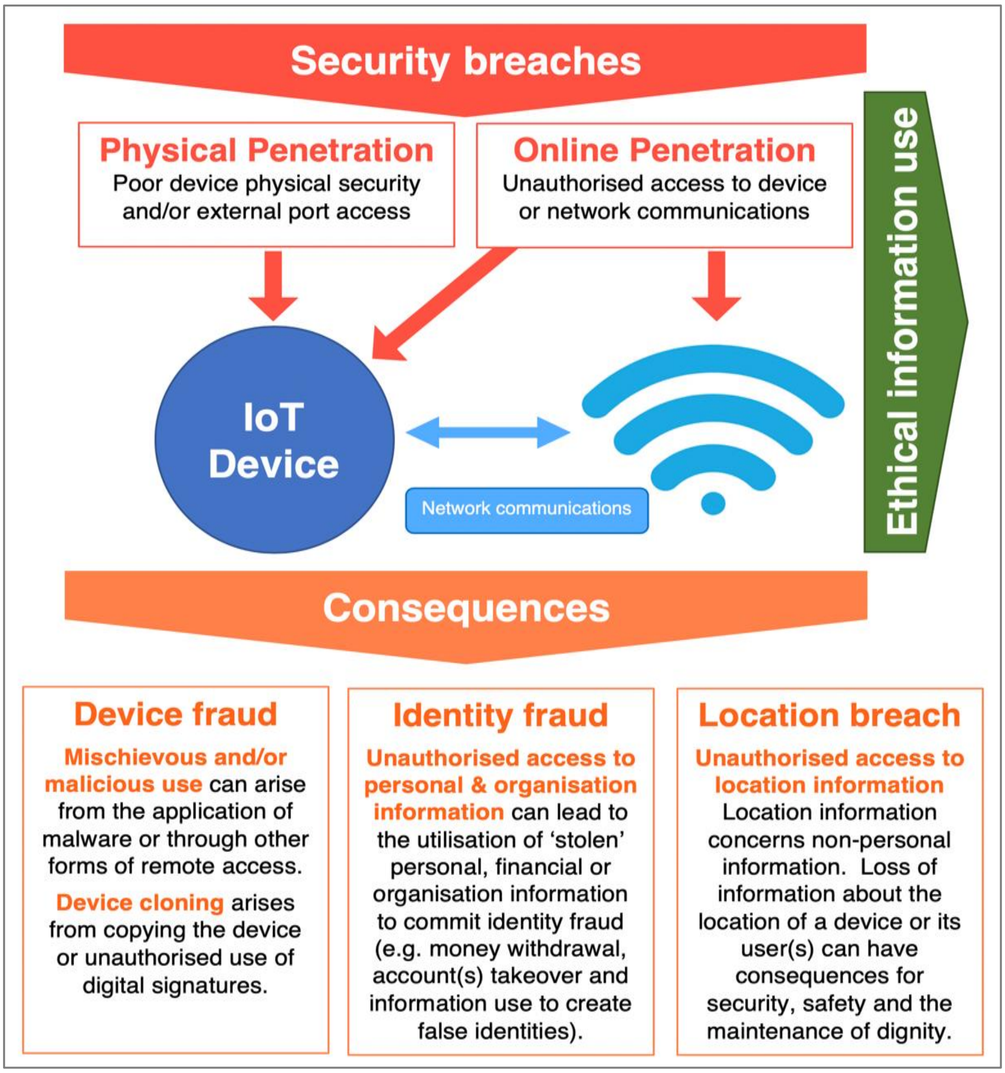
3.2 Conceptualisation of radio equipment security risks, consequences and solutions

3.2.1 Conceptualisation of security breaches and their impacts

A common feature of EU industrial product legislation is the importance of a risk-based approach in determining whether legislation is needed, and if yes, how this might best be dealt with through harmonised technical standards. In the case of the RED, and this specific study, to develop an understanding of the risks, the logic of risk assessment in information security has been followed. This takes as a starting point the need to identify and analyse the threats, vulnerabilities and the perceived impacts of device-level beaches occurring.

To understand key issues concerning the security of radio equipment (RE), the study team has therefore developed a conceptualisation framework for security breaches that can affect RE, technical solutions that could prevent such breaches, and an assessment of the potential consequences should a breach occur. Figure 3.2 below provides an overview of the conceptualisation.

Figure 3.2: Conceptualisation of radio equipment security breaches and consequences


Security breaches
Physical Penetration
Poor device physical security and/or external port access
Online Penetration
Unauthorised access to device or network communications
Ethical information use
IoT Device
Network communications
Consequences
Device fraud
Mischievous and/or malicious use can arise from the application of malware or through other forms of remote access.
Device cloning arises from copying the device or unauthorised use of digital signatures.
Identity fraud
Unauthorised access to personal & organisation information can lead to the utilisation of 'stolen' personal, financial or organisation information to commit identity fraud (e.g. money withdrawal, account(s) takeover and information use to create false identities).
Location breach
Unauthorised access to location information
Location information concerns non-personal information. Loss of information about the location of a device or its user(s) can have consequences for security, safety and the maintenance of dignity.

The primary focus of the conceptual framework is on identifying the main risks relating to connected RE products and wearables, and the consequences of security breaches, with a view to assessing which technical solutions would best reduce the risks, thereby preventing such breaches from occurring in the first place. An example in this regard is the integration of data protection by design and by default principles into the GDPR, and the development of good practice guidance, codes of conducts and the emergence of technical standards on security by design and by default principles, which extend more broadly than data protection and privacy by design and default, but which contribute towards achieving the objectives of the latter.

In addition, the purpose of the analysis of risks and the impacts of breaches is to provide an input to the policy options analysis (Section 4.3) to determine which of the policy options defined would prevent breaches from occurring, thereby optimising risk mitigation. It is also important that personal data and information knowingly provided by radio device users (including consumer IoT products) is used and stored in an ethical manner and respects data protection principles set out in the GDPR, the applicable legislation.

The research has also investigated the magnitude of impacts arising from security breaches and methods to prevent unauthorised access and misuse of radio equipment. Ethical issues are considered in Section 3.2.4.

3.2.2 Security breaches and solutions

Growth in radio equipment and the Internet of Things (IoT) is forecast to provide numerous benefits and business opportunities. However, there are risks associated with radio equipment. 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. The two key types of security breaches are:

- **Physical penetration:** Physical security weaknesses arise when an attacker can disassemble a device and/or access the storage medium and data stored on that medium. Breaches can also occur when USB ports or external ports are used to access a device; usually using features intended for configuration or maintenance.
- **Online penetration:** Online penetration vulnerabilities arise in the network services that are used to access radio devices that allow an intruder to gain unauthorised access to wireless and fixed network communications or associated data. A common weakness is the unencrypted exchange of data between radio devices.

3.2.3 Solutions: Preventing breaches

Nearly all security breaches can be overcome by adhering to ***Security by Design and Default*** principles. This approach to software and hardware development 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. The approach ensures security is 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 as an afterthought.

Through the targeted consultation, manufacturers were asked how they ensure the security by design and default requested by the GDPR in all products that they place on the market. More than half of those responding use international standards to guide the security of their product development, whereas others relied on internal procedures; however only 22 respondents answered in total.

In relation to the reliance on international standards, respondents expanded by highlighting the following specific standards:

- ISO/IEC 27000 series, which is not linked to a sector but is relevant for connected devices, e.g. ISO-IEC 27001.
- IEC 62443-X series, e.g. IEC 62443-4-1, which specifies the process requirements for the secure development of products used in industrial automation and control systems.
- ISO 26262, addressing the functional safety of electrical and/or electronic systems in automobiles.
- ETSI TS 103 645, addressing cybersecurity for the consumer Internet of Things.

Considering the second point, a number of organisations are also developing guidelines and Codes of Practice for radio equipment and IoT security[33]. These guidelines highlight a number of methods to prevent breaches. For the two key types of breach these include:

Physical penetration

- **Minimise exposed attack surfaces:** All devices and services should operate on the 'principle of least privilege;' unused ports should be closed, hardware should not unnecessarily expose access,

[33] ANEC, Danish Standards Authority, ENISA (EN 303 645), DIN, ETSI, UK Department for Digital, Cultural and Media Studies (Code of Practice for Consumer IoT Security), ISO/IEC JTC 1/ SC 27/WG 4 and EuroSmart.

services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate;

- **Make systems resilient to outages:** Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, considering the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power;
- **Ease of device installation and maintenance:** Installation and maintenance IoT devices should employ minimal steps and should follow security best practices on usability. Consumers should also be provided with guidance on how to securely set up their device.

Online penetration

- **No default passwords:** Passwords should be unique and not resettable to any universal factory default value;
- **Keep software updated:** Software components in radio devices should be securely updateable;
- **Securely store credentials and security-sensitive data:** Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable;
- **Communicate securely:** Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely;
- **Ensure software integrity:** Software on devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function;
- **Ensure that personal data is protected:** Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR) [34]. In accordance with GDPR principles, the organisations acting as data controllers must provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes. Good practice stemming from developing guidelines and Codes of Practice for radio equipment and IoT security would suggest that device manufacturers and IoT service providers should also provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes;
- **Monitor system telemetry data:** If telemetry data is collected from devices and services, such as usage and measurement data, it should be monitored for security anomalies;
- **Easy personal data deletion:** Devices and services should be configured in a way that enables personal data to be easily removed when there is a transfer of ownership, when the consumer wishes to delete the information and/or when the consumer wishes to dispose of a device;
- **Validate input data:** Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices should be validated.

General protection measures

- **Vulnerability disclosure policy:** Companies that provide internet-connected devices and services should provide a public point of contact as part of a vulnerability disclosure policy in order to

[34] GDPR requirements will operate when those collecting information become ‘controllers of personal data’. This will probably arise for most, but not for all ,radio devices.

enable security researchers and others to report issues. This should complement extensive ongoing efforts by the information security community to monitor and document vulnerabilities, as illustrated in the box below.

Box 3.1: Case study insight: Vulnerability monitoring and documentation

Common vulnerabilities are monitored and documented extensively by the information security community. A prominent example is the Common Vulnerabilities and Exposure (CVE) database, which is sponsored by the US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and maintained in collaboration between technology and cybersecurity organisations (e.g. Lenovo, Cisco, MITRE, Trend Micro, Panasonic etc.), research institutions, government departments, academics and other security experts.

"The process of creating a CVE Entry begins with the discovery of a potential security vulnerability or exposure. The information is then assigned a CVE ID by a CVE Numbering Authority (CNA), a Description and References are added by the CNA, and then the CVE Entry is posted on the CVE website"[35]

An important additional design principle, which is incorporated into the GDPR as 'data minimisation', is not to collect unnecessary personal information or sensitive data. Only data critical to the functionality of a radio device should be collected and all data collected should be de-identified or anonymised and properly protected with encryption.

These simple preventative measures will usually prevent security breaches and overcome the three types of consequences described in Section 3.2.5.

3.2.4 Consequences of security breaches

The orange boxes in the lower part of the Figure 3.2 conceptualisation provide an overview of the potential consequences that will arise if security breaches arise.

Any regulatory initiative through either the RED or alternative EU-level policy or regulatory actions should focus on minimising the risks of security breaches. If these can either be prevented or at least minimised, then the consequences outlined in this section will not materialise or be of less severity than would otherwise be the case. The possible activation of delegated acts pertaining to data protection and security and protection from fraud should therefore focus on preventing security breaches; for instance, through the setting of baseline security requirements, and adherence to security by design and default principles. It should however be recalled that whilst steps can be taken to strengthen security by IoT device manufacturers, prevention is extremely difficult with any connected device; and the aim of technical solutions is therefore on improving resilience and a strengthening of mitigating efforts rather than on providing guaranteed security, which would not be realistic, given the ever-changing nature of the threat.

However, further research is needed to determine whether the types of security breach are common across all connected RE product categories, or whether specific products pose specific risks. This would then have implications for the types of technical solutions that could be developed, including under a regulatory scenario, harmonised technical standards.

Nonetheless, Figure 3.2 focuses on three key types of consequences. These include:

- **Device fraud:** This type of fraud arises if unauthorised users are able to access radio devices for mischievous and/or malicious reasons. Unauthorised access can enable the installation of malware to deny or change access and functionality of a device, and ransomware to threaten

[35] Common Vulnerabilities and Exposures (CVE) website. Last accessed on 29.11.2019 at: http://cve.mitre.org/cve/identifiers/index.html#creation

‘publication’ of personal information or data. An additional threat could be to change the use of a device (e.g. to “mine” cryptocurrencies).

  - Device fraud can also arise from cloning or copying the device or unauthorised use of digital signatures. A pertinent example is Near Field Communication (NFC) skimming on smart phones, watches and other devices to enable unauthorised payments and purchases. Cloning of automated electronic fee collection devices on toll roads have also been reported. [36]
  - Unauthorised access or jamming of radio equipment to impair or incapacitate functionality can also be problematic. The most high-profile example during the last decade has concerned the possible life-threatening consequences of security breaches to cardiac pacemakers.[37]

- **Identify fraud:** Identity fraud occurs from the unauthorized use of one’s identity and/or data associated with an identity for fraudulent purposes. Identity fraud vulnerabilities during data transfer generally arise from poor design and the transmission of data over insecure networks.[38]
- **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 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 whilst on holiday and it is therefore essential such information is anonymised and that any information identifying the location the data is transmitted from is secured on a server that cannot be accessed by staff from the service provider.

3.2.5 Conceptualisation of data misuse and its impact

It is important to highlight that whilst improvements in security could prevent data breaches at the device level (covered by the RED) to avoid data protection and privacy being compromised, this is only part of the picture in that there is also the crucial question as to what types of personal data is being collected by manufacturers and other EO in the value chain, such as technology providers as well as service providers that serve as data processors as defined in the General Data Protection Regulation (GDPR). It should be noted that further information regarding the legal requirements in relation to data collection and processing and the ethical dimension of data and information use by manufacturers is provided in Section 3.3.2.

Among the crucial considerations conceptually are what types of personal data (or identifiers) are being collected by EO, for what purpose, and whether GDPR rules relating to data minimisation and the need for consent to be obtained from data subjects are being complied with.

Evidently, in a big data era, smart devices are collecting ever-more personal data, as well as identifiers (such as IP addresses) that are also considered as personal data under the GDPR as the individual user can potentially be identified, or at least personal information about them such as their location.

There are important issues around whether the GDPR has led to behavioural changes among manufacturers (in their capacity as data controllers and whether other data processors in the value chain, such as chip and components manufacturers as well as software and app developers that are data processors are complying with GDPR since it came into effect in May 2018 or do dubious business practices that could risk compromising personal data protection and privacy persist in relation to smart internet-connected RE devices. Examples from the case studies as to the extent to which

[36] https://www.rfidjournal.com/articles/view?15224/2

[37] https://www.wired.com/2008/03/scientists-demo/

[38] Pal, A. The Internet of Things (IoT) – Threats and Countermeasures. https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures.

manufacturers are collecting data legitimately and in accordance with the GDPR are provided in Section 4.2.4.

3.3 Analysis of existing EU legislation and regulatory gaps

In this section, the baseline situation regarding existing EU legislation to ensure data protection and privacy, and protection from fraud in internet-connected radio equipment and wearable RE are considered. The extent to which there are any regulatory gaps in the current EU legal framework is also analysed, considering the RED and wider relevant EU legislation.

3.3.1 Mapping of relevant EU legislation

Several relevant pieces of EU legislation and non-legislative initiatives have been identified, drawing on the Commission's inception impact assessment (January 2019) and wider feedback. These are:

- **The General Data Protection Regulation (GDPR) 2016/679** – concerns data protection and privacy in the processing of personal data in general. Also requires data controllers to ensure that the processing of personal data is secure by design and default (Art. 25);
- **The ePrivacy Directive (e-PD) 2002/58/EC -** concerns the processing of personal data and the protection of privacy in the electronic communications sector
- **The proposed ePrivacy Regulation** 2017 is a regulatory proposal to update the currently applicable e-PD. The aim is to reform the existing 2002 legislation to adapt the ePrivacy rules to new technological realities, and to align them with the 2016 GDPR. A 2019 version is currently under revision by the Council and as a result of drafting suggestions made in various EU Presidencies[39];
- **The EU Cybersecurity Act (CSA) -** establishes an EU-wide cybersecurity certification framework for digital products, services and processes. The Act came into force on 27th June 2019;
- **Non-Cash Payments Directive (EU) 2019/713 -** combating fraud and the counterfeiting of non-cash means of payment. This could have relevance in terms of shedding light on a definition of fraud for Article 3(3)(f) protection from fraud; and
- **Regulation (EU) 2017/745 on Medical Devices (MDR) and Regulation (EU) 2017/746 –** whilst medical devices are outside study scope , the recast Directive is the first time in EU industrial product legislation that steps were taken to strengthen security for high-risk product categories where security vulnerabilities have been identified (e.g. the risk of devices such as pacemakers being hacked[40]). The aim is to ensure data protection and privacy of such devices is improved.

Before being able to determine whether the two DAs in the RED (Art. 3(3)e on data protection and privacy and Art. 3(3)f respectively on protection from fraud) should be activated, a central issue is how far existing EU legislation provides adequate legal protection for consumers and businesses in terms of ensuring adequate safeguards relating to data protection and privacy, and protection from fraud in connected RE devices and wearables.

Furthermore, the extent to which there are any gaps, loopholes or inconsistencies in the existing EU legislation is also explored. Key issues are now considered in the table on the following page:

[39] The e-Privacy Regulation is a proposal for greater regulation of electronic communications within the EU to increase privacy for individuals and entities.

[40] https://www.wired.com/story/pacemaker-hack-malware-black-hat/

Table 3.6: Analysis of existing EU legislation - relevance to strengthening security (data protection and privacy and protection from fraud)

Legislation	Scope	Relevance to the RED	Key legal issues and extent of regulatory gaps, loopholes and/ or inconsistencies
The General Data Protection Regulation (GDPR)2016/679	• Generally applicable to the collection and processing of personal data from individuals after products are placed on the market. • However, Art. 25, data protection by design and default applies both at the time of the determination of the means and at the time of processing to achieve high levels of data protection.	• The GDPR sets out rules relating to data protection and privacy, which must be implemented by data controllers at the time of the design of processing and that processing actually takes place. • **Art.25[41] data protection by design and default** imposes obligations on the data controller: • **Before and after products are placed on the market: Art. 25(1)** [....]. The data controller shall implement, both at the time of the determination of the means and at the time of processing itself, appropriate technical and organisational measures, such as pseudonymisation, to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of this Regulation and protect the rights of data subjects. • **Before and after post-product placement on the market. Art. 25(2).** The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. • **Article 35 requires Data Protection Impact Assessments (DPIA) to be undertaken in specific cases**, a process that helps organisations identify and minimise risks that result from data processing. DPIAs are usually undertaken when introducing new data processing processes, systems or technologies that are likely to result in a high risk to the rights and freedoms of natural persons. The DPIA is a new requirement under the GDPR. • **Art. 40 (Codes of Conduct)** and **Art. 41[42] (Monitoring of approved codes of conduct)** of the GDPR set out detailed	• However, since the obligation in Art.25 is addressed to data controllers, there is arguably a case for imposing similar requirements for products being placed on the market by manufacturers (in particular when they are not acting themselves as data controllers in respect of the processing of personal data) to strengthen the legislation's effectiveness, as the GDPR and RED could act together in concert., • GDPR provides specific obligations for data controllers and data processors respectively and is applicable both before, and after, products are placed on the market. • A regulatory gap is arguably that the GDPR addresses data controllers and processors explicitly, whereas neither manufacturers or technology providers are explicitly mentioned in the Regulation's articles as needing to implement specific measures to ensure data protection and privacy safeguards or features ensuring protection from fraud prior to products being placed on the market **as a condition of market access**. • The lack of explicit mention of manufacturers means that there are two different scenarios. Manufacturers and technology developers may fall within the GDPR's scope when they play an active role in the intended processing of personal data from which they derive commercial profits. For instance, they may act as controllers/joint-controllers with other third-party service providers and/ or data analytics businesses by determining the purposes and means of processing. For example, if they install hardware or more likely software into a product with a view to facilitating data collection and the selling of personal data to third parties. In such instances, manufacturers would be subject to the full rigour of the GDPR (e.g. consent, transparency in data collection, data protection by design

[41] Art. 25 GDPR - data protection by design and by default. https://gdpr-info.eu/art-25-gdpr/

[42] Art. 41 GDPR, Monitoring of approved codes of conduct. https://gdpr-info.eu/art-41-gdpr/

Legislation	Scope	Relevance to the RED	Key legal issues and extent of regulatory gaps, loopholes and/ or inconsistencies
		provisions regarding the development of voluntary codes of conduct at a sectoral level. This provides a means of demonstrating GDPR compliance, which is an example of how voluntary codes can play a role in contributing to the effective implementation of data protection legislation. • Responsibility for the enforcement of data protection legislation lies with national data protection authorities. Any legislation adopted under the RED related to data protection must respect such responsibility.	and default). • However, if they are not directly involved in the collection and processing of data, but only in the design and manufacturing of the product, then they do not fall under the GDPR's scope, which constitutes a legal gap. • Under the GDPR, there is the possibility for national DPAs to impose large fines on companies for data breaches. • There can be maximum fines of individual companies or organisations of up to 20 million euros or 4% of the global annual income of the company depending on the severity of the data breach and the company's cooperation with the pertinent bodies. The current regulatory proposal in respect of the ePrivacy Regulation has adopted the same level of sanctions to ensure alignment with the GDPR. However, fines often relate less to device-level security and more to the unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. • Such breaches may take place for example in the transmission and storage of data or could occur at a network level and / or in a data centre. • Under the GDPR, whereas there is the possibility for DPAs to impose significant fines, there are no legal powers for MSAs to remove connected RE products from the market that do not respect users' data and privacy and their obligations under the GDPR, for example if they are non-secure. • This means that that consumers and business users are not adequately protected, as connected RE products and wearables that could potentially compromise data protection and privacy or provide inadequate protection from fraud remain on the market. • Overall, the GDPR offers some protection (esp. through Art. 25 and related articles such as Art. 35 on DPIA for high-risk technologies) but does leave gaps in regulatory enforcement as described above.

Legislation	Scope	Relevance to the RED	Key legal issues and extent of regulatory gaps, loopholes and/ or inconsistencies
ePrivacy Directive (Directive 2002/58/EC)	• Applicable after products have been placed on the market	• Similarities in the Directive's objectives and underlying rationale for the possible activation of a delegated act under Art. 3(3)(e). • Recital 5 states that "advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user". • Recital 46 states that "[…] It may be necessary to adopt measures requiring manufacturers of certain types of equipment used for e-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[43] (the R&TTE Directive) and mutual recognition of their conformity will ensure that the introduction of technical features of e-communication equipment including software for data protection purposes is harmonised to be compatible with the implementation of the internal market.	• The ePD also needs to be updated to reflect the evolution in the EU legal framework, in particular, to bring the Directive into line with the GDPR. The proposed Regulation has still not been adopted (see row below). • The Directive concerns e-communications after products have been placed on the market, whereas the RED sets out the essential requirements that must be addressed prior to products being placed on the market.
ePrivacy Regulation (currently at proposal stage being reviewed by Council)	• Concerns the transmission of personal data using e-communications.	• ePrivacy Regulation (ePR) - Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). • First draft of ePR was published as proposal on 26 October 2017. The Parliament adopted an amended draft and voted in favour of negotiations with the Commission and Council. On 5 December 2017, the then EU Council presidency published its own draft, which was followed by further drafts. The Romanian presidency presented its draft on 22 February 2019; the latest drafts of July this year and most recently of 4 October 2019 were produced by the current Finnish presidency of the Council. These drafts are still being negotiated in the Council. • As no final regulatory text is available, it is difficult to analyse fully. However, among the relevant changes are extending the application of the right to confidentiality of communications to all communication service providers.	• The ePR's scope covers both content and metadata derived from electronic communications – both will need to be anonymised or deleted if users have not given consent, unless required for billing purposes. • As is the case with the GDPR, whilst the ability to levy administrative sanctions in the form of fines will serve as a deterrent to companies that breach privacy rules, the legislation is aimed at service providers rather than directly at other relevant actors within the value chain, i.e. manufacturers. • The issue of consent fatigue has been raised in finalising the draft legislation i.e. making users select privacy settings whenever new privacy options are available. • Under the latest version of Article 8 of the Regulation, the use of technologies such as cookies to collect information from end-users' "terminal equipment" (devices) or to use the

[43] The R&TTE Directive was part of the alignment package of 8 Directives that were brought into line with the New Legislative Framework in 2014, and the R&TTE Directive became the now applicable RED 2014/53/EU

Legislation	Scope	Relevance to the RED	Key legal issues and extent of regulatory gaps, loopholes and/ or inconsistencies
		• The proposal aims to update the rules in Directive 2002/58/EC(4), and to create new possibilities for providers to process communications data, and ensure that traditional and internet-based communication providers are bound by the same rules when it comes to respect for the confidentiality of communications and to reinforce trust and security in the Digital Single Market (DSM). The proposed Regulation will complement the GDPR as regards e-communications data that qualify as personal data and will seek to ensure consistency with GDPR. • There are differences in the applicability scope compared to the ePD to reflect market developments. The ePR will be applicable to 'over the top' (OTT) service providers (e.g. WhatsApp, Facebook, Gmail and Skype and not just telecommunications service providers). • As is already the case with infringements under the GDPR, companies face substantial fines if they breach the draft ePrivacy Regulation. The ePR cites the GDPR provisions with regard to rules on legal remedies, liability and penalties. The stipulation on administrative fines (Article 23 of the draft), for example, refers to Art. 83, GDPR. Depending on the nature of the infringement, fines may amount to EUR 20,000,000 or 4% of the company's worldwide annual turnover, whichever is higher (Article 23(3) of the draft). • In previous drafts, Art. 10 contained a requirement for software (including browsers) to offer the option of preventing third parties storing information on end-user equipment. On installation, the end-user had to be informed about the privacy settings options and required to select their settings in order to complete installation. This was suggested by the European Data Protection Supervisor, but has been deleted in the Directive's current draft. There were going to be requirements around the granularity of technical settings to enable user control, and for a requirement that privacy settings should be set at their highest level by default.	processing and storage capabilities of those devices is prohibited unless: *inter alia "It is necessary for security, fraud prevention or detection of technical faults in a time limited capacity"*. • Under the old definition of consent, there was confusion about whether consent to cookies and their equivalents could be implied (opt-out) or had to be explicit (opt-in), with EU MS taking differing approaches. It is clear that consent now has to provide an unambiguous indication of the data subject's wishes so inaction or silence will be insufficient, however, questions around how to capture specific consent remain. • Consent is also defined in the GDPR and part of the rationale for updating the e-PD into the e-PR is the need to align the legislation with the GDPR (including definitions). • The ePR will help to ensure that personal information on their computer, smartphone or tablet can only be accessed with their permission.
The Cybersecurity Act (CSA) 2019[44]	Voluntary Cybersecurity Certification scheme.	• The CSA was adopted in 2019 and has created a voluntary framework for European Cybersecurity Certificates for products, processes and services. • Although this is the first internal market law that takes up the challenge of enhancing the security of connected products, IoT devices and critical	• Voluntary certification scheme only, without any mandatory requirements. • Given non-mandatory, MSAs do not have legal powers to remove products from the market.

[44] https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

Legislation	Scope	Relevance to the RED	Key legal issues and extent of regulatory gaps, loopholes and/ or inconsistencies
		infrastructure through such certificates. • The creation of such a cybersecurity certification framework incorporates security features in the early stages of their technical design and development (security by design). • A certification-based approach implies a non-mandatory approach. A key issue will be the extent to which – and how - cybersecurity could be strengthened as a horizontal theme if the two delegated acts were to be activated, and the role of voluntary certification therein. • ENISA will assist Member States in establishing and implementing vulnerability disclosure policies (Art.6(b), albeit on a voluntary basis). In time, this could allow a detailed understanding of the nature and scale of vulnerabilities, by RE product group, at the national and EU level. • Whilst some principles mentioned in ETSI TS 103645 are included in the approach to the development of certification schemes under the CSA, not all are likely to be. • Some stakeholders perceive that CSA certification schemes are likely to be more relevant to ensuring cybersecurity in B2B products, such as ensuring information security in high-speed telecommunications (e.g. ahead of rolling out of 5G networks). However, ENISA is also considering development of a certification scheme for consumer IoT devices.	• It will take considerable time to roll out certification schemes across different product groups, as well as vulnerability disclosure policies. • Some similarities with some of the rules outlined in the GDPR e.g. Art. 25 GDPR data protection by design and default has been translated into the principles contained within the CSA (e.g. Article 51 - security by design and by default are both mentioned as parts of the objectives of the future cybersecurity schemes). •
Regulation (EU) 2017/745 on Medical Devices (MDR) and Regulation (EU) 2017/746	Manufacturers explicitly required to take IT security measures, including in relation to hardware and software	• The risks associated with such devices from a security perspective, in terms of hacking vulnerabilities, have been recognised, with manufacturers explicitly required to put in place appropriate IT security measures[45]. • Art. 17(4) Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended. • Annex I "Safety and Performance Requirements", of the MDR requires manufacturers to consider the risks associated with the possible negative interaction between software and the IT environment. It also requires the principles of development life cycle, risk management, including	• The Directive provides a useful illustration of how security in relation to device hardware and software might be regulated, but it only covers the risks associated with connected RE embedded in medical devices rather than other types of RE falling within the RED's scope). • The requirements in respect of the protection and confidentiality of personal data only cover investigational devices.

[45] MDR came into force on May 25th 2017. Manufacturers of currently approved medical devices will have a transition time of three years until May 26th 2020 to meet the requirements of the regulation.

Legislation	Scope	Relevance to the RED	Key legal issues and extent of regulatory gaps, loopholes and/ or inconsistencies
		information security, to be considered[46]. - There are also requirements specifically relating to the protection and confidentiality of personal data. However, these only relate to certain types of products for the investigational devices covered by Article 62. - CHAPTER II - Documentation regarding applications for Clinical Investigation (pg. 175 of the MDR, point 4.5) sets out the requirements for data protection and confidentiality of personal data for investigational devices[47].	
Non-cash payment Directive (EU) 2019/713 [48]	Not directly related to industrial products.	- Not directly related to industrial products, but provides useful general principles relating to outlawing different types of online frauds. - Although the Non-Cash Payments Directive does not define fraud and the counterfeiting of non-cash means of payment, it suggests that a harmonised definition should cover new types of non-cash payment instruments that allow for the transfer of electronic money and virtual currencies.	- Concerns computer-related fraud rather than RE. - Not directly applicable to manufacturers, but some basic principles and definitions relating to preventing fraud are potentially useful.

[46] Putilov, D. (2018). How Cybersecurity Requirements will engage Medical Device Manufacturers in the Future. *VDE*, August 16, 2018. https://www.vde.com/en/dgbmt/working-areas/cybersecurity-requirements-medical-device-manufacturers

[47] Under the MDR, the following must be provided for investigational devices: Description of the arrangements to comply with the applicable rules on: 1) organisational and technical arrangements that will be implemented to avoid unauthorised access, disclosure, dissemination, alteration or loss of information and personal data processed; 2) a description of measures that will be implemented to ensure confidentiality of records and personal data of subjects; and 3) a description of measures that will be implemented in case of a data security breach in order to mitigate the possible adverse effects.

[48] 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/legal-content/EN/TXT/?qid=1557838897143&uri=CELEX:32019L0713

As the concept of data protection by design and default is especially important in the context of this IA, below we provide an overview of the requirements set out in Article 25 below.

Art. 25 GDPR - Data protection by design and by default

1. Taking into account state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, **implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles,** such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. [1]The controller shall implement appropriate technical and organisational measures for ensuring that, by default, **only personal data which are necessary for each specific purpose of the processing are processed. [2]That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.** [3]In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Examples of key issues in implementing data protection by design and default, and some of the relevant issues around what obtaining consent might mean of possible usefulness to the RED, were the two Delegated Acts to be activated are provided below:

Box 3.2: GDPR – considerations as to how far the legislation is fit for purpose to regulate data protection and privacy in an IoT context

The GDPR is centred on a risk-based approach. In order to demonstrate compliance, there is a stress on integrating data protection and privacy by design and default principles. There is also an emphasis on only collecting personal data for specific purposes, and not further processing it for incompatible purposes.

Two scenarios are considered in this case study. Under the first scenario, the manufacturer has no intention to collect and share personal data (and derives no commercial benefits from such practices). If it has not implemented sufficient data protection and security by design requirements and the product could be used/hacked by third parties to collect personal data (without the manufacturer's intention, participation, or benefit), this is an important scenario in which the manufacturer would not directly fall within the scope of the GDPR. This arguably therefore constitutes a legal gap.

A second scenario would fall under the GDPR. New business models are emerging relating to internet-connected RE products and devices, especially in consumer IoT, to capitalise on the "big data" and the monetisation of big data analytics. In the case of Smart TVs, software may be embedded on the product prior to it being placed on the market which gathers detailed information about personal viewing habits and then sells on this data to third parties, sharing some of the revenue with TV manufacturers. By doing so, the manufacturer of the Smart TV would be considered to have become a data controller (or as a joint controller with the app provider), since it would have decided on the collection and sharing of personal data by integrating software that allows such data collection and sharing.

The issue of user consent which is embedded in the GDPR would help protect the user of a Smart TV as there would be a need to ensure that such data is being collected with users' explicit consent when they first set-up the product, if it is already pre-loaded.

In line with the regulatory approach adopted under the GDPR, in the drafting and finalisation of the ePrivacy Regulation, there is an issue as to how far software and service providers should explicitly require users' consent explicitly. It can also be noted that consent has already been defined in the GDPR in Article 4(11)[49].

A related issue is the trade-off between requesting user consent to ensure their privacy isn't compromised and over-doing consent requests such that it would be cumbersome for the user[50].

Linked to this is the question of the pseudonymisation of personal data and information required in Art. 25 GDPR, which is different from the "anonymisation" of personal data and information. Pseudonymous data still allows some form of re-identification (even indirect and remote), while anonymous data cannot be re-identified. *"Pseudonymisation techniques differ from anonymisation techniques. With anonymisation, the data is scrubbed for any information that may serve as an identifier of a data subject"*[51].

If such data is gathered about product usage, and this data is anonymised, this would be GDPR-compliant. A more nuanced area is the collection of data where user preferences result in personal data being used in order to target suggested media and advertising to users. This arguably has benefits for the consumer (seeing more relevant content customised to their personal interests) but also raises data protection and privacy considerations. Where the manufacturer would play a role in the collection and processing of personal data, for example by integrating in the product software allowing data collection and sharing from which it would derive commercial benefits, it is likely to be considered as a data controller and would need to abide by all requirements under the GDPR and ePrivacy legislation. This includes assessing what information about product usage could legitimately be collected and retained by the manufacturer, and what data could be used in order to personalise content to individual users, and under which conditions.

A challenge from a legal perspective is that there may be some grey areas, as the use of AI and big data is relatively new. For example, good practices developed by national data protection offices suggest practices such as anticipating risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals and using privacy-enhancing technologies (PETs) to assist in complying with data protection by design obligations. However, if say in the case of a Smart TV, the connected RE product is preloaded with software that automatically monitors viewers viewing habits, this may go against such principles.

Manufacturers could however take steps themselves to protect consumers. For example, they could set users' profile settings to the most privacy-friendly setting by default. Moreover, if manufacturers/service providers/software developers wish to collect personal data of users and share them with third parties to harness the commercial potential of big data, they would likely become a data controller of such data processing and would need to abide by all the requirements in the GDPR and in ePrivacy legislation. This would include the requirement to obtain appropriate consent for their monitoring of data about their product usage and sharing such data with designated third parties for specified purposes.

One of the issues raised in a few stakeholder interviews is the challenge in determining who within the value chain is responsible if data is misused. Several different actors may be involved in collecting big data for data analytics purposes for a given connected RE product, such as the manufacturer, a third-party data analytics company, and a service provider via an application downloaded on to the device. Whilst there may be some perceived ambiguities as to the delineation of responsibility for data collection and processing – and any resulting data breaches – this appears to be addressed clearly in the GDPR, as there is a clear distinction and definition provided of the responsibilities of data controllers and processors.

[49] Consent of the data subject means any 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.

[50] https://cms.law/en/deu/insight/e-privacy

[51] https://gdpr.report/news/2017/11/07/data-masking-anonymisation-pseudonymisation/

Ultimately, data controllers remain responsible for the collection and processing of data, although it is true that there can be considerable complexity, for instance if the manufacturer is a data controller for collecting some types of data, but third party app providers may also be data controllers for data collected via the device via an app. A further complexity is that some organisations may outsource their data processing and will need to ensure GDPR compliance throughout their supply chain and demonstrate how they will handle their data securely and responsibly. However, there was no feedback from industry associations or individual manufacturers that this has proven especially problematic.

It has been pointed out in a recent article[52] that data controllers must be vigilant in ensuring GDPR-compliance across the value chain as *"Data breaches in one area could be detrimental to all other business within the supply chain, from both a financial and a reputation perspective. Consequently, organisations will need to carry out the appropriate due diligence and monitor suppliers to ensure they are GDPR-compliant".*

However, it also suggests a number of good practices to help manage GDPR compliance across the value chain, such as:

Recording flows of personal data throughout the supply chain, including third party suppliers and distributors to identify where personal data is being received and stored.

- Examine internal practices to ensure that processes are in place which enable your company to satisfy the 72-hour breach notification requirement. Investigate whether your current insurance policies will cover data protection and security breaches, including any breaches made by suppliers
- Review existing supplier contracts that involve the processing of personal data to ensure they cover all the data protection provisions necessary under the GDPR.

The question as to whether managing GDPR implementation across the supply chain in connected radio equipment products could perhaps however be among the issues considered in the forthcoming 2020 evaluation of the GDPR, to double-check that this is not problematic for industry.

The overall findings from the assessment of regulatory gaps are presented under Policy Option 1, which considers the status quo option of relying on existing EU legislation. However, it is worth summarising a few findings from the above assessment in brief:

- Existing EU legislation addresses data protection and privacy through a horizontal framework , for instance, in relation to what types of data can legitimately be collected from users (under the GDPR), the need to respect privacy in data processing (GDPR) and the need to ensure privacy in the transmission of data via electronic communications (the e-Privacy Directive).
- This means that while processing via internet-connected radio equipment devices and wearable RE falls within the general scope of the GDPR and the e-PD, but this still leaves regulatory gaps, as there may be some regulatory gaps in relation to the processing of personal data in products and radio-equipment devices where the manufacturer or technology provider would not act as a data controller or as a data processor, as well as gaps in enforcement in such cases.
- Moreover, GDPR compliance is not a condition of market access, which means that although data controllers could be fined once the product is already on the market, there are gaps in enforcement powers in terms of the ability of market surveillance authorities to remove products from the market.
- Whereas strengthening security has the potential to stop device penetration and thereby to prevent breaches of personal data and privacy, and thereby lower the risk of fraud, the GDPR already covers risks relating to data misuse by data controllers and processors, and the need for a

[52] Source - Preparing Your Supply Chain for GDPR, May 2018

valid legal basis to process data from users of connected radio equipment.

- Whilst the GDPR addresses data protection by design and default in Art. 25, this is targeted at data controllers, and indirectly at processors. Other EO in the value chain – manufacturers and technology providers are only explicitly mentioned in the recitals, although if they decide to collect personal data, they may well have to define themselves as data controllers, and thereby fall within the Regulation's scope.
- The ePrivacy Directive also affords users of connected radio equipment privacy in the transmission of e-communications via telecoms networks from their mobile device and via the internet. If the current text of the ePrivacy Regulation proposal is adopted, then it will extend protection with clearer definitions of consent, in line with the GDPR (Art. 4(11)).
- Current EU legislation does not however address the problem of combatting fraud either generally or when using connected RE devices and wearables. This appears to be a regulatory gap, although some stakeholders questioned whether the RED is the optimal legal means of addressing fraud, as it is already covered in national criminal law. Nonetheless, the increasing prevalence of instances of online fraud, including of connected radio equipment devices, suggests that there is a regulatory gap.
- Another legal gap is that even if the two delegated acts were to be activated, these would only cover wireless products, and not wired. According to the findings from the desk research, and the two online consultations, this would only cover approximately 60-80% of the market. Moreover, there are a further set of security vulnerabilities that exist irrespective of whether the product remains connected to the internet or not i.e. beyond internet-related vulnerabilities, there are offline vulnerabilities too, e.g. data being stolen via memory stick or hard drive from a physical laptop device. However, these vulnerabilities are outside the scope of the RED.
- In the case of fraud, whilst the focus of this IA is on wireless devices, it could be the case that data is stolen offline, and then used online. Evidently, here, no cybersecurity standard could prevent such an occurrence even if the delegated acts were activated, although basic steps could be taken to prevent such data theft e.g. requiring two-step authentication.

3.3.2 Legal requirements in relation to data collection and processing and the ethical dimension of data and information use by manufacturers

The primary tenets of information security are: ensuring confidentiality (i.e., accessed only be authorized users), integrity (i.e., trustworthiness of data) and availability of data (i.e., accessible when needed).

A relationship exists between law and ethics. In some instances, law and ethics overlap and what is perceived as unethical is also illegal. In other situations, they do not overlap. In some cases, what is perceived as unethical is still legal, and in others, what is illegal is perceived as ethical. A number of recent newsworthy ethical issues concerning the use of data by Facebook and other organisations have highlighted this dichotomy.

A number of organisations have prepared 'ethical data frameworks'[53] and 'guidelines'[54] that provide basic ground rules that could be used to promote the ethical use of data obtained from radio equipment. The guidelines focus on ethical issues concerning data collection and use. Some guidelines

[53] Information Accountability Foundation. 2015. Unified ethical frame for big data analysis. http://informationaccountability.org/wp-content/uploads/IAF-Unified-Ethical-Frame-v1-08-October-2014.pdf

[54] European Data Protection Supervisor. 2015. Towards a new digital ethics: Data, dignity and technology. Opinion 4/2015 https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf Taylor et al. 2017. Public sector data ethics: From principles to practice.

acknowledge the important mandatory role of applicable data protection law, such as the General Data Protection Regulation (GDPR) , when those collecting data become ‘controllers of personal data’.

Where devices and/or services collect and process personal data, they must do so in accordance with existing EU legislation, namely the GDPR and the ePrivacy Directive 2002. Ethical codes of conduct in such cases should not replace compliance with legal requirements laid down in the law. Certain practices relating to data collection and processing fall under GDPR (especially when there is processing of personal data by an organisation). Under the GDPR, there are specific tools to facilitate compliance with the law, which are Codes of conduct approved by a national data protection authority (DPA), certification, and guidelines from the EDPB and national DPAs. Therefore, whilst tools and guidance on ethical issues in data collection may be useful, they are not a substitute for, or guarantor of compliance with the law, which is at the heart of some of the data misuse issues raised in this section.

There are a number of overriding considerations and common principles relevant to connected radio equipment. These include:

- **Transparency on data collection and uses:** Transparency is a legal requirement in the GDPR. In recent years, prior to the GDPR coming into effect, users were often unaware or uncertain as to what data was being collected about them (or their device), how it would be used, or what it may reveal about the data subject. This could be particularly invasive when multiple data sources are combined, allowing seemingly benign data collection to be used in ways that are not acceptable to the user. Many of the potential solutions, such as letting data subjects know when and why data is being collected or allowing users to access what a company knows about them, are covered by the GDPR. If an organisation wishes to utilise the data previously collected, they fall under the GDPR and must amongst others comply with legal requirements of information in Art. 12-14 GDPR. The complementary use of Codes of Conduct under Article 40 of the GDPR can contribute to the prevention of data misuse. Codes of conduct that facilitate compliance with GDPR must undergo a specific process under the GDPR in that they must be approved by a competent DPA. Only those codes have legal validity to guide against data misuse as defined in the GDPR, rather than any code put forward by industry.
- **Fairness:** Regarding the legal situation, when individuals are asked by an organisation to share their data, the data controller falls under the GDPR’s scope and all requirements under the GDPR are applicable. Fairness is defined in Art.5 GDPR which links to the need for a lawful legal basis to carry out the processing and transparency requirements in the GDPR.
- An example was identified from the case studies of software pre-loaded onto Smart TVs which collects data about users’ viewing habits. The issue arises as to whether explicit consent is being requested from the user to monitor their viewing habits and whether they are aware that such data is being collected for marketing purposes.
- **Data protection by design and default** is a legal requirement in Article 25 GDPR. It requires organisations acting as data controllers to implement, both at the time of the determination of the means for processing and at the time of the processing itself, appropriate technical and organisational measures to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects.
- **Practical integration of GDPR into internet-connected RE products and other industrial products.** Whilst Article 25 of the GDPR introduces the principle of data protection by design, its “technologically neutral” approach ultimately offers no guidance on how data protection can be designed into technology.[55] Technological and organizational solutions ensure compliance with

[55] Urquhart, L., Lodge, T., and Crabtree. (2019). Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology*, 27(1), 1-27.

laws and help increase user trust in data controllers. These solutions can be in the form of privacy engineering and the adoption of privacy-enhancing technologies (PETs).[56] The only technological and organizational measures mentioned in the GDPR are pseudonymization and certificate mechanisms (the latter of which has not yet been initiated).[57] In fact, the GDPR does not include a clear obligation for the adoption of privacy-enhancing technologies (PETs) and privacy engineering.[58] Rubenstein and Good (2019) identified hard and soft PETs:[59] Hard PETs treat data controllers as untrustworthy by designing technology with data minimization in mind and minimizing the distribution of this data. Soft PETs treat data controllers as trustworthy and give them the authorization to implement data management practices that give users the tools they need to make informed choices about their data use. According to Rubenstein and Good (2019), privacy engineering can be in the form of "privacy by architecture" (i.e., the design of technology with the minimization of data collection in mind through the use of technical means, such as hard PETs) or "privacy by policy" (i.e., data management notices and soft PETs).[60]

- Article 25 of the GDPR does not impose any obligations on the developers of technology to implement technological and organizational data protection measures. While not included in the substantive provisions of the GDPR, Recital 78 of the regulation states: *"When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."*

Case study insight: GDPR and Transparency in practice

As illustrated through the case studies conducted on specific product groups, many companies have taken steps with regard to improving transparency, since GDPR came into application in May 2018,. For instance, with regard to laptops (see Annex 9 for the full case study), large companies have implemented measures to allow and empower users to have control of how their personal data is used. For example, Microsoft's privacy dashboard allows users to manage browser data, location data, data collected by Cortana (Microsoft's personal digital assistant) and more.[61] Apple, in a similar fashion, have implemented a range of measures to preserve user privacy across its range of applications, including Intelligent Tracking Prevention in the Safari web browser, not linking location to a user's Apple ID, and use of end-to-end encryption on iMessage.[62]

Many of the issues identified above relate to the question of how effectively those involved in the value chain are implementing the GDPR. Since 25 May 2018, there has been a growing list of fines and notices levied under the GDPR, which support implementation practices and operational behaviours. In particular, it is worth noting that many, and indeed the most-high profile, of these fines have been related to the implementation by organisations of insufficient technical and organisational security

[56] Rubinstein, I. S. and Good, N. (2019). The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default. *International Data Privacy Law*, https://doi.org/10.1093/idpl/ipz019.

[57] Finick, M. (2019). Smart contracts as a form of solely automated processing under the GDPR. *International Data Privacy Law*, 9(2), 78-94.

[58] Rubinstein, I. S. and Good, N. (2019). The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default. *International Data Privacy Law*, https://doi.org/10.1093/idpl/ipz019.

[59] Rubinstein, I. S. and Good, N. (2019). The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default. *International Data Privacy Law*, https://doi.org/10.1093/idpl/ipz019.

[60] Rubinstein, I. S. and Good, N. (2019). The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default. *International Data Privacy Law*, https://doi.org/10.1093/idpl/ipz019.

[61] https://account.microsoft.com/account/privacy?refd=privacy.microsoft.com&destrt=privacy-dashboard

[62] https://www.apple.com/fr/privacy/

measures. This illustrates two simple, but important facts: i) many companies are getting it wrong in terms of their approach to data protection and to ensuring adequate device-level security to ensure data protection and privacy; and ii) actions are being taken by national DPAs EU to identify and challenge these business behaviours. Some prominent examples are included in the box below.

With this in mind, there is a strong consumer protection dimension in terms of how far the GDPR may change business behaviours and operational practices specifically in respect of EO within the value chain in sub-sectors relating to connected RE. For example, manufacturers are not explicitly addressed in the GDPR, only implicitly.

One of the difficulties in examining to how effective existing legislation such as the GDPR is in preventing illicit data collection and data misuse by manufacturers, third parties, technology providers and service providers is that there is only a relatively small body of case law available at this stage in monitoring and enforcement of GDPR implementation. No cases appear to directly relate to manufacturers yet. Examples of case law falling under Art. 25 and Art. 35 GDPR, are provided in the CBA under the assessment of the costs of data breaches. Further selected examples of GDPR fines and notices issued are provided below.

GDPR fines and notices: Examples

- Selected examples of the issuance of fines under the GDPR by Data Protection Authorities (DPAs), which apply data protection law at national level in EU Member States, are now provided. In some cases, DPAs have issued fine as a result of companies publicly admitting to a data breach and then putting in place mitigating measures. In other cases, complaints have been received (e.g. from consumer associations, individuals) and DPAs have taken action upon investigation. Some DPAs appear to have been more proactive than others in this regard, in terms of whether they adopted a proactive or a reactive approach. This matters as only when there has been a reasonable critical mass of case law are such cases likely to have a stronger deterrent effect on data controllers ultimately responsible for data processing (including in relation to personal data collected through internet-connected RE products and devices).
- Intention to issue a large fine issued against British Airways by the UK Information Commissioner's Office (ICO) for 'poor security arrangements' in relation to the protection of log in, payment card, travel booking and name and address data.
- €180,000 fine issued against Active Assurances by the French Commission Nationale de l'Informatique et des Libertés (CNIL) for the implementation of insufficient security measures to protect the personal data of users.
- €645,000 fine issued against Morele.net by the Polish DPA, Urząd Ochrony Danych Osobowych (UODO) due to a lack of appropriate technical and organisational measures that led to the leakage of personal data, including personal ID numbers (PESEL number).

3.3.3 Data protection and privacy in the context of connected radio equipment and wearables

The baseline legal situation in respect of data protection and privacy at EU level was described above. In this sub-section, literature has been identified looking at issues specifically concerning how data protection and privacy legislation and key principles are implemented in the context of the IoT.

The GDPR came into effect on 28th May 2018 and it has not yet been evaluated how effective it has been overall. A particular area that could be interesting from the perspective of the RED in a future evaluation study is to ascertain how far having such legislation in place has led to changes in market practices among EO, especially producers of internet-connected RE products and devices to ensure greater attention to data protection by design and default. Addressing the issue of whether EU legislation such as the GDPR and the proposed ePrivacy Regulation are sufficient to address data protection and privacy concerns in relation to the design of internet-connected RE products and devices is difficult to do comprehensively until evaluation materials become available. Nevertheless, to the extent that academic literature and research in grey literature was available, this issue has been examined at least in part through this study. Interviewees also had views on this issue, notwithstanding the limitations imposed by the absence of a detailed evaluation of GDPR implementation at this stage.

A range of relevant literature has been identified in regard to the challenges in implementing privacy and data protection legal requirements in an IoT context (see the bibliography in Annex 1 for a full list). Selected examples of the most relevant points raised are provided in this section.

Consent: A report by the Information Commissioner's Office (ICO) – the UK's DPA – on GDPR implementation in a big data context[63] notes whilst the law is written in a clear way, there are nevertheless **practical implementation challenges** in translating requirements regarding consent into operational business practices. This is especially the case in the context of the growing use of **Artificial Intelligence (AI) and big data analytics** to analyse product usage and to predict and personalise content accordingly using personal data and information.

Some literature points to the **inherent tensions between the GDPR requirements relating to the proportionality of data collection** on the one hand, and **big data-driven business models** in the context of internet-connected radio equipment and wearables. This was an issue identified for example in the case study on Smart TVs (Annex 9). The case study research found that software to monitor users' viewing habits is often integrated onto the TV prior to sale and that when the TV is first activated, users may not be aware of ongoing monitoring of their viewing and that they have given their consent. This raises privacy considerations, even if their rights are legally protected due to the requirement for data controllers to secure consent unambiguously.

The GDPR's Article 5(1)(c) states that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" i.e. proportionate (the 'data minimisation' principle). A report by the ICO in the UK acknowledges this tension. *"Big data analytics tends to involve collecting and analysing as much data as possible, and in many cases all the data points in a particular set, rather than a sample ("n=all")". "The issue regarding data minimisation is not simply the amount of data being used, but whether it is necessary for the purposes of the processing, or excessive"*[64]*.*

Other literature points to the general challenge in the GDPR of the obligation for **data controllers to ensure Data Protection by Design**. For example, a study[65] on Data Protection by Design and Technology Neutral Law notes that *"This is a new type of legal concept, whereby law aligns itself with the earlier ethical and policy-oriented concept of Privacy by Design".* The challenges inherent in implementing privacy by design principles have also been alluded to in other literature, including that pre-dating the GDPR[66].

In addition, other literature provides an examination of the **threats to privacy posed by particular technologies**, some of which are connected radio equipment and wearables. For instance, a book on

[63] The Data Protection Act and General Data Protection Regulation - Big data, artificial intelligence, machine learning and data protection, UK's ICO. Available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[64] Data Protection Act and General Data Protection Regulation - Big data, artificial intelligence, machine learning and data protection, 2017.https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[65] Data Protection by Design and Technology Neutral Law, Mireille Hildebrandt, Radboud University Nijmegen, Laura Tielemans, Vrije Universiteit Brussel.

[66] Ann Cavoukian, Privacy by Design .. Take the Challenge (Ontario: Information and Privacy Commissioner of Ontario (Canada), at https://ozone.scholarsportal.info/bitstream/1873/ 14203/1/291359.pdf, 2009); Demetrius Klitou, 'Privacy by Design and Privacy-Invading Technologies: Safeguarding Privacy, Liberty and Security in the 21st Century', Legisprudence 5, nr. 3 (2011):

safeguarding privacy[67] identifies a number of technologies that raise issues around privacy and the ethical aspects of data collection wherever this may be intrusive. It points to the following examples: body scanners, public **CCTV microphones** and CCTV loudspeakers, and **human-implantable microchips (RFID implants) that provide geolocational data.** The book shows “how and why laws that regulate the design and development of privacy-invading technologies (PITs) may more effectively ensure the protection of privacy than laws that only regulate data controllers and the use of such technologies”. This is supported by case studies focusing on four specific PITs. This is a crucial point relevant to the present IA in that it implies that the GDPR would be more effective if supported by supporting regulations translated into technical solutions (such as harmonised standards) to help translate the GDPR rules in a way that ensures that manufacturers and EO in the value chain are explicitly made responsible for ensuring data protection and privacy, rather than indirectly so.

Other literature supports the idea that, given the principle of data protection by design and default in the GDPR is general and legally-binding, *“as the need arises, regulations for specific technological contexts should be adopted which require embedding data protection and privacy principles into such contexts"*[68]. Although the report dates from 2013, it is supportive of the idea of introducing technical legislation to specify data protection principles in different technological contexts, such as industrial products through the delegated acts foreseen in the RED.

Furthermore, the GDPR’s Article 35 requires **Data Protection Impact Assessments (DPIA)** to be carried out before the deployment of high-risk technologies by data controllers. This article underpins the “protection by design” principle in Article 25. It is consequently of strong relevance to IoT products and devices. Guidance and templates have been developed by some national data protection authorities (DPAs) to assist organisations in carrying out such a DPIA[69].

A further piece of research published in a Law Journal[70] notes that one of the problems associated with ensuring privacy in an IoT context is that developments in big data analytics are emerging rapidly and this can make it difficult to determine:

- What type of data are being collected via smart devices and for what purpose?
- Whether the purpose for which the data is originally being collected and processed might when combined with other data sources be used for ancillary purposes without the knowledge of the data subject, even if initial permission has been given to collect the data or monitor smart product usage.

The article in the above journal notes that *“Most communications between smart devices occur automatically, potentially without the user being aware of it. Many questions arise around the vulnerability of the devices in the IoT, often deployed outside a traditional IT structure and lacking sufficient built-in security. The IoT demands consideration and research into how to best balance the opportunities that the IoT affords against legal risks it imposes on data protection. Considerable questions about how our currently existing EU framework for protection of personal data applies in IoT are being raised”.*

[67] Demetrius Klitou (2011) Privacy by Design and Privacy-Invading Technologies: Safeguarding Privacy, Liberty and Security in the 21st Century, Legisprudence, 5:3, 297-329

[68] Data Protection Working Party, 02356/09/EN, WP 168, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009, p. 3.

[69] Templates on developing a DPIA from CNIL in France: https://www.cnil.fr/en/privacy-impact-assessment-pia

ICO guidelines in the UK, *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/*

[70] Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things’ (2015) Information & Communications Technology Law 24/3, 262-277.

Issues around how users of connected radio equipment and wearables value their privacy can be factored into the cost-benefit assessment (see Section 4.3).

3.3.4 Protection from fraud in the context of connected radio equipment and wearables

Whereas there is extensive literature on the GDPR and data protection and privacy, there is more limited academic research available on the issue of fraud, which is often linked to data breaches and problems in respect of data protection and privacy.

Research has been undertaken for example into identity-related fraud. A study from the UK[71] found that "identity crimes (also Wall, 2013) costs the UK taxpayer about £1.2 billion per year (NFA, 2012:10) and losses are increasing each year". "Whether malicious or unintended, the fact is that personal and corporate information falls intentionally into criminal hands. The study debates what constitutes personal identity, whether a complete identify is needed or only an identifier". Evidently, the rapid rise of the IoT means that there are greater risks of fraud as consumers and businesses are using ever more connected RE products and devices in their daily lives.

In terms of the **numbers of users affected**, the 2019 Identity Fraud Study[72], developed by Javelin Strategy & Research, found that a record high of 16.7 million consumers were victims of identity fraud in 2017; although this fell to 14.4 million in 2018. Regarding the **costs associated with these incidents,** the same report states that victims' out-of-pocket fraud costs in fact more than doubled between 2016 and 2018, hitting $1.7 billion.

There appear to be **two key drivers underpinning the levels of fraud** described above: (i) a lack of industry preparedness; and (ii) highly organised and effective fraudsters.

Considering the first point, technology companies and commentators have regularly noted that the rapid emergence of the IoT and the significant (current and future anticipated) growth in the number of IoT and internet-connected RE devices and products has resulted in manufacturers creating insecure products. This is due in part to pressure to bring those products to market quickly[73] and a lack of understanding of the related security issues[74], including the protection of personal data and privacy as described above and protection against fraud.

On the demand side, there is also a lack of awareness of possible security vulnerabilities. According to a survey by Aruba, an HP Enterprise company, 84% of businesses had already experienced an IoT-related security breach.[75] However, by 2019, the report noted that 85% of responding businesses reported that they would have implemented an IoT strategy.[76]

Regarding the second point raised above, it is regularly reported that fraudsters operating in this space are highly organised, innovative, effective, well-resourced and business-minded with a desire to provide a high-quality 'service' to their own customers. In this respect, these fraudsters can gather intelligence and attack in a variety of ways and with varied tools. For instance, fraudsters may use "disruptive mechanisms, spyware, password snatchers, legitimate device imitators" and other tools

[71] Future Identities: Changing identities in the UK – the next 10 years, DR 19: Identity Related Crime in the UK, David S. Wall, Durham University, January 2013.

[72] Javelin Strategy & Research, 2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt, 6 March 2019. https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt

[73] CSO Online, Opinion: Fraud and the Internet of Things, contributed by Rahul Pangam, 6 July 2017. https://www.csoonline.com/article/3206164/fraud-and-the-internet-of-things.html

[74] WeDo Technologies, Blog: Identifying IoT fraud risks: The challenges for operators, blog by Luis Brás, https://blog.wedotechnologies.com/identifying-iot-fraud-risks-the-challenges-for-operators

[75] Aruba, a Hewlett Packard Enterprise company, White Paper: IoT and the smart digital workplace: Opportunities and challenges, 2018, https://www.arubanetworks.com/assets/wp/WP_SmartDigitalWorkplaceIoT.pdf

[76] Pipeline, What we need to do in the fight against IoT fraud and identity theft, contributed by Rui Paiva, 2019, https://www.pipelinepub.com/security_and_assurance/IoT-security

to gather the intelligence necessary to conduct payment fraud, account takeover and identity theft. Furthermore, they rely on the inability of organisations to respond to and recover from cyber-attacks. More specific examples of methods to commit fraud in the context of internet-connected RE devices and products are detailed in the box below.

Box 3.3: Fraud in the context of internet-connected RE devices: Examples

As part of the October 2016 Mirai attack, nearly 150,000 **smart security cameras**, **routers and other IoT devices** were infected with malware.[77] First, the Mirai botnet was used to launch a Distributed Denial of Service (DDoS) attack against the French host OVH, in a bid to prevent the use of a popular tool that players of the game Minecraft utilised to fight DDoS attacks against their servers. Subsequently, the code for the Mirai botnet was posted online by its author and used elsewhere, including in a significant attack against Dyn, an internet infrastructure company.[78]

In the insurance world, there are a few examples of **tracking data from internet-connected RE devices being used by insurers** to drive positive user behaviour and to set policy premiums. For instance, a life insurance provider in the US offered up to 15% off its policy premiums if customers proved they were living a healthy lifestyle by providing data to the company via a smart wearable device. Fraudsters could exploit an insecure device to steal data from individuals with healthy lifestyles and re-use or sell those data to secure improved policy premiums. Another example relates to insurance in the automotive industry. Tracking metrics on driving safety has been used to provide customers with discounted policy premiums. As for the health data above, driving data could be stolen from safe drivers and re-used by or sold to unsafe drivers in order to get better insurance deals.[79]

Contactless payments are another environment where fraud has been significantly debated in relation to internet-connected RE devices. As detailed by Mastercard, “the [contactless] cards and devices contain an embedded chip and a radio frequency (RFID) antenna that provide a wireless link with the contactless reader. When the card or device is tapped against the reader, information is transmitted in a highly secure manner within a fraction of a second.”[80] Contactless payments are on the rise, but levels of adoption differ across the EU. For instance, UK Finance reported that 7.4bn contactless payments were made in the UK in 2018, increasing 31% on 2017, and 69% of UK adults now use contactless payments.[81] According to Statista, contactless payments are similarly popular in the Netherlands, with 51% of all card transactions in 2018 now contactless.[82] On the other hand, this source reports that only 4% of all Belgian card transactions and only 3% of all Portuguese card transactions are contactless.

Although there has been much debate online regarding the possibility of ‘skimming’ (i.e. initiating payments without the knowledge of the card holder), there are many security measures in place to

[77] CSO Online, Opinion: Fraud and the Internet of Things, contributed by Rahul Pangam, 6 July 2017. https://www.csoonline.com/article/3206164/fraud-and-the-internet-of-things.html

[78] CSO Online, Feature: The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet, contributed by Josh Fruhlinger, 9 March 2018. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

[79] Pipeline, What we need to do in the fight against IoT fraud and identity theft, contributed by Rui Paiva, 2019, https://www.pipelinepub.com/security_and_assurance/IoT-security

[80] Mastercard, Beyond the Transaction, Dispelling the Myths: The Reality about Contactless Security, contributed by Ryan Erenhouse, 17 January 2018, https://newsroom.mastercard.com/2018/01/17/dispelling-the-myths-the-reality-about-contactless-security-2/

[81] UK Finance, Rise in mobile banking and contactless as consumers take pick ‘n’ mix approach to payments, 6 June 2019, https://www.ukfinance.org.uk/press/press-releases/rise-mobile-banking-and-contactless-consumers-take-pick-n-mix-approach-payments

[82] Statista, Contactless payments market share at POS in Europe 2018, by country, 11 November 2019, https://www.statista.com/statistics/946228/contactless-payments-market-share-at-pos-in-europe-by-country/

prevent this process; not least that Chip & PIN machines need to be registered with a payment vendor and linked to a bank account, where every transaction is monitored for fraudulent activity.[83] Furthermore, only limited information (account information, not including the three digit security code, and a one-time code) is transmitted to the Chip & PIN machine by the card or device (e.g. smart phone, smart watch). As such, commentators consider the likelihood of such attacks to be low.

The main risks in relation to contactless payment cards and devices are: i) the possibility of using certain applications to read the account number and expiration date from the card; and ii) the ability to use the card without user verification, if the card is physically lost or stolen. In this respect, it was reported by Action Fraud, the UK's national reporting centre for fraud and cybercrime, that, in 2018, instances of theft relating to contactless cards doubled over a 10-month period, rising from 1,440 cases worth £711,000 to around 2,740 cases worth nearly £1.8m.[84] However, considering the above points, the vast majority of these cases relate to the theft or loss of contactless payment cards.

In terms of mitigating the risk of fraud, there are a range of measures that can be taken on both the manufacturer and consumer sides. For manufacturers and service providers, **product and service risk assessments** can be used to assess the risks of fraud related to a specific product and the associated services and, on that basis, devise a holistic security strategy that appropriately considers all technology, people and process risks.[85] Within such assessments, the key question in relation to fraud is how to differentiate between legitimate and fraudulent customers, which requires authentication of users in real-time. In this respect, digital identity technologies are considered an important mechanism to detect fraudulent users. Such technologies assess a user actions against a digital identity develop by the company on the basis of historical data collected on that user, including, for example, device, identity and behaviour data.[86]

In addition, other data can be utilised to query and authenticate users within a fraud management system, as illustrated by the following list of fraud protection solutions related to card fraud:

- "**Geolocation:** Verify the location of the customer with the actual location of the active card.
- **Biometric analysis:** Compare the customer's fingerprint with that of the cardholder.
- **Address verification service:** The issuer compares the addresses provided during the transaction.
- **CVV:** Additional credit card security code required during the final payment authorization.
- **IP intelligence:** Deep analysis of the IP address used for the transaction to monitor possible risks associated with this location.
- **Device intelligence:** Deep packet inspection and proxy piercing capabilities to expose specific identifying details of the connected device submitting the transaction.
- **Three domain secure:** A cardholder authentication protocol for e-commerce transactions and [card not present (CNP)] purchases. XML-based protocol designed to be an additional security layer for online security in card-based transactions.
- **Merchant co-op:** New orders are compared against millions of orders taken by other merchants

[83] Finextra, Blog: 5 Myths of contactless payment security, 1 December 2018, contributed by Rik Coeckelbergs, https://www.finextra.com/blogposting/16365/5-myths-of-contactless-payments-security

[84] Independent, Online article: 'Contactless' fraud cases double in 10 months, contributed by Kate Hughes, 11 January 2019, https://www.independent.co.uk/money/spend-save/contactless-card-fraud-increase-money-security-bank-account-a8722361.html

[85] WeDo Technologies, Blog: Identifying IoT fraud risks: The challenges for operators, blog by Luis Brás, https://blog.wedotechnologies.com/identifying-iot-fraud-risks-the-challenges-for-operators

[86] Techradar, Online article: Evolution of fraud in the IoT era, contributed by Alisdair Faulkner, 22 August 2018, https://www.techradar.com/news/evolution-of-fraud-in-the-iot-era

contributing in-network and scrubbed for fraud risk.

- **SSL:** Secure encrypted communication protocols between devices and payment solutions."[87]

On the consumer side, the Identity Theft Resource Center (ITRC)[88] maintain a number of resources in this regard. Amongst its recommendations, the ITRC stats that consumers should:

- Ensure connected RE devices are only purchased from a "reputable manufacturer with a track record of providing secure devices"[89];
- Isolate devices on their own protected networks;
- Ensure universal plug-and-play is disabled on routers;
- Change any default passwords included in a device;
- Ensure devices are only used on a home network with a secured Wi-Fi router (i.e. not on public Wi-Fi);
- Ensure devices are updated with new security patches, when released.

Furthermore, once a device will no longer be used, ensure that it is decommissioned effectively. The ITRC suggests using e-recycling initiatives that will help reduce the impact of electronic waste but also ensure devices are comprehensively cleaned of user data.

3.3.5 National and international developments in addressing the security vulnerabilities in connected RE products/ devices and wearables

There have been a number of regulatory and non-regulatory developments at national and international levels to address different types of security vulnerabilities identified in connected RE products/ devices and wearables wherever inadequate safeguards in respect of data protection and privacy and protection from fraud when consumers and businesses use connected RE devices and wearables have been identified. Examples are now presented from the UK and the US:

- **Non-regulatory developments.**

Voluntary approaches to addressing cybersecurity concerns in IoT and other smart devices could range from a purely self-regulatory approach, to using voluntary tools and instruments as a mechanism to complement the implementation of new mandatory requirements. The types of instruments concerned vary from the development of codes of conduct by and/ or for industry to awareness-raising measures among manufacturers, industry more broadly and citizens as to how to strengthen cybersecurity in the manufacturing and use of IoT devices and smart products.

Examples are the development of voluntary codes of practice relating to consumer IoT security for manufacturers of IoT devices in the UK, and the development of baseline security requirements for IoT device manufacturers, for instance by NIST in the US.

- **Regulatory developments**.

Several regulators globally are considering whether it is necessary to regulate vulnerabilities in IoT devices and products to strengthen basic cybersecurity functionality in consumer IoT devices. Examples are:

- At EU level, the present study focusing on connected radio equipment and wearables falling within the scope of the RED, and the possibility of activating the two Delegated Acts foreseen in Articles

[87] Verifi, Online article: Internet of Things – Boosting your fraud protection, https://www.verifi.com/in-the-news/internet-things-boosting-fraud-protection/

[88] Identity Theft Resource Center, https://www.idtheftcenter.org/privacy-and-identity-theft/

[89] Pipeline, What we need to do in the fight against IoT fraud and identity theft, contributed by Rui Paiva, 2019, https://www.pipelinepub.com/security_and_assurance/IoT-security

3(3)(e) and 3(3)(f).

- At national level in the UK. The UK's DCMS is considering regulating consumer IoT devices, having piloted a voluntary approach previously.
- Internationally, in the U.S. California has already adopted a law on consumer IoT cybersecurity. There have also been attempts to legislate at a U.S. federal level, but these have not yet come to fruition. Moreover, California has also introduced legislation similar to the GDPR regarding the collection and use of personal data by companies. This came into effect in January 2020.

The above-mentioned developments are now explored in greater detail.

3.3.6 National developments in the EU and third countries

This section considers selected regulatory and non-regulatory developments at national level in the EU-28. It should be noted that as regulation of connected RE devices and wearables is a new and emerging area, there are only selected examples to date, mainly from the UK.

The UK[90] provides an example of a **voluntary approach at national level**, although consideration is being given as to whether minimum (mandatory) baseline requirements should be introduced to complement this in the near future. In 2018, DCMS, the UK Government department issued a **Code of Practice (CoP) for Consumer Internet of Things (IoT) Security for manufacturers**[91]. The CoP aimed to improve baseline security and to advance an industry-wide 'security by design' approach which encourages manufacturers to "develop IoT devices with security as a central component of its use, rather than working backwards to try and create security measures via software updates or other tactics[92]". The code of practice includes for example, a proposal for unique passwords for all IoT products which are made non-resettable to any universal factory setting.

It also requests that a public point of contact is added for the product manufacturer and details of the minimum length of time that products will receive regular security updates.

The code considers some of the good practice principles set out in **ETSI TS 103 645**, a cybersecurity standard for consumer IoT devices, which is designed to establish a security baseline for internet-connected consumer products and to provide a basis for the development of future IoT certification schemes. The standard was developed by the ETSI Technical Committee on Cybersecurity. It has been analysed as a possible technical solution that could be utilised, were the delegated acts pursuant to Art. 3(3)(e) and Art. 3(3)(f) to be activated (see Policy Option 3 – a regulatory approach in Section 4.1.5).

Supporting methodological guidance on **'security by design' and 'privacy by design' principles was also developed**. Separate (and more practical) guidance was developed for consumers to ensure high levels of cybersecurity for smart devices being used at home. The guidance was developed by the DCMS working in conjunction with the National Cyber Security Centre (NCSC) and drew on feedback from industry, consumer associations and academia. The guidance was published in draft in March 2018 (final version in November 2018).

An **industry code of conduct is not mutually exclusive with a regulatory approach**, since a code of conduct could set out common sense principles important to cybersecurity and could exist with, or

[90] There are similarities in developments at EU level, in that security by design and default feature strongly in guidance developed by ENISA at EU level and by DCMS.

[91] DCMS published the Code of Practice for Consumer IoT Security to support all parties involved in the development, manufacturing and retail of consumer IoT, October 2018.

[92] Daube, Nitzan. (2019). Regulating the IoT: Impact and new considerations for cybersecurity and new government regulations. *Help Net Security*, April 11, 2019. https://www.helpnetsecurity.com/2019/04/11/iot-regulation-2/

without supporting legislation. Therefore, in 2019, DCMS subsequently launched a consultation[93] on the security of consumer IoT regarding the possibility of a regulatory approach. This ran from May 1st 2019 to June 9th 2019. The consultation put forward three different options to consultees, namely:

- **Option A: Mandatory IoT security label on consumer IoT products.** Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self-declare and implement a security label on their consumer IoT products;
- **Option B: Mandatory use of minimum of three guidelines principles from the Code of Practice for IoT Security and the ETSI TS 103 645.** Under this option, retailers would only sell consumer IoT products that adhere to the top three guidelines, with the burden on manufacturers to self-declare that their consumer IoT products adhere to the top three guidelines of the Code of Practice for IoT Security and the ETSI TS 103 645; and
- **Option C: Mandatory use of all thirteen guidelines.** Mandate that retailers only sell consumer IoT products with a label that complies with all 13 guidelines of the DMCS Code of Practice (which itself is closely related to the good practice principles in the ETSI standard), with manufacturers expected to self-declare and to ensure that the label is on the appropriate packaging.

The results have not yet been published, but work is ongoing by DCMS to gather data on the scale of the problem by mapping the IoT security landscape and costing the impacts of a regulatory approach.

An example of how a voluntary regulatory approach could support the full and effective implementation of EU legislation is the GDPR (Regulation 2016/679)[94]. Under Articles 40 and 41, there are provisions within the GDPR for the development of **sector-specific certification and codes of conduct ("codes")** relating to data protection as a mechanism to support the legislation's implementation. The provisions in codes *"represent a practical, potentially cost-effective method to achieve greater levels of consistency of protection for data protection rights. Codes can act as a mechanism to demonstrate compliance with the GDPR. Notably, they can help to bridge the harmonisation gaps that may exist between Member States in their application of data protection law"*[95].

3.3.7 Regulatory developments in the US

It is also worth briefly summarising developments outside the EU internationally in other regulatory jurisdictions. For example, in the **US,** there have been two attempts to introduce mandatory requirements for consumer IoT security, the first at federal level, and the second in California at state level. At a federal level, the **IoT Cybersecurity Improvement Act 2017** was proposed, but didn't succeed in 2017. However, the **IoT Cybersecurity Improvement Act of 2019** has been newly-introduced in Congress. The law is now being debated again.

Presently, in the U.S., there is an absence of a national standard for IoT security and each company must therefore decide how they will ensure the security of connected devices they produce. U.S. lawmakers were seeking to address this shortcoming in the 2017 Act, which would then require any IoT devices that the federal government uses to meet a bare minimum of security standards. The 2019 Act went further by requiring these IoT devices to comply with the IoT security recommendations[96] of

[93] UK Department for Digital, Culture, Media & Sport. (2019). Consultation on regulatory proposals on consumer IoT security. https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security.

[94] The General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all individual EU citizens and those of the European Economic Area (EEA).

[95] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 by the European Data Protection Board , pg. 4 - https://edpb.europa.eu/sites/edpb/files/consultation/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf

[96] NIST. (2019). NIST Releases Draft Security Feature Recommendations for IoT Devices. https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices

the National Institute of Standards and Technology (NIST). Indeed, NIST has also held a publication consultation from July – September 2019 to solicit feedback on the baseline requirements[97] developed for IoT devices targeted at IoT Device Manufacturers. A parallel can be drawn here with the development of baseline requirements by ENISA in consumer IoT devices.

Both versions of the legislation only apply to government procurement, although this could have a significant demonstration effect by encouraging IoT device manufacturers to build-in IoT security. The proposed 2019 Act mandates contractual provisions for government agencies buying IoT devices. As such, the provisions are stronger and more detailed than state level legislation, such as the California bill mentioned below, **Senate Bill 327,** but they apply only to Federal Government buyers.

There have been a number of other attempts at federal level to introduce legislation that could help to strengthen IoT security, but the bills concerned have not passed. These include: the **Securing IoT Act** of 2017, which would make the Federal Communications Commission add cybersecurity standards when authorising wireless equipment; the **IOT Consumer TIPS Act of 2017** that would require the "Federal Trade Commission to develop cybersecurity resources for consumer education and awareness regarding the purchase and use of devices that are part of the IoT;" the **SMART IoT Act of 2017** that would require the Department of Commerce to **conduct a study on the state of the IoT industry; the DIGIT Act of 2017**, which would require a federal working group to provide a **report to Congress on the current state of the IoT industry, including the regulatory environment, security and data protection, consumer protection, and the current government use of IoT;** and the **Cyber Shield Act of 2017**, which would require the Department of Commerce to create a **voluntary grading system for IoT device security.** If the Cyber Shield Act passed, the expectation was that an easily-understandable consumer labelling system would show consumers how a device rated in cybersecurity terms.

At the state level, **California** has adopted legislation to regulate consumer IoT security[98] ahead of the federal level initiative through Senate Bill 327. The legislation introduces security requirements for connected devices sold in the US. It defines them as any device that connects directly or indirectly to the internet and has an IP or Bluetooth address.

From January 1, 2020, a manufacturer of a connected device would be 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".* The definition of what constitutes a "reasonable security feature" has attracted some controversy among US stakeholders.

An interviewee commented that the adoption of this new regulation ought to have a positive effect in changing market behaviours as a whole. California is often at the forefront of regulatory developments at state level, and a significant-scale economy in its own right. The legislation adopted in California conveys the message that manufacturers, wholesale distributors and retailers should not sell products that are not adequately cybersecure. This was viewed as potentially having a positive signalling effect on the market. It was also seen as likely that others may adopt a similar approach as California, but on a voluntary basis rather than through state legislation.

The California Consumer Privacy Act (CCPA) becomes effective on January 1, 2020. In common with the GDPR, it allows consumers to see what data companies are collecting about them and also allows them to request that companies delete or do not sell their personal data. The CCPA's penalties have

[97] Fagan, M., Megas, K. N., Scarfone, K. and Smith, M. (2019). Draft NIST IR 8259 2 Core Cybersecurity Feature Baseline 3 for Securable IoT Devices: 4 A Starting Point for IoT Device Manufacturers - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf

[98] Badbury, Danny. (2018). California bill regulates IoT for first time in US. *Naked Security*, September 13, 2018. https://nakedsecurity.sophos.com/2018/09/13/california-bill-regulates-iot-for-first-time-in-us/

been capped at $7,500 per consumer. The potential fine can only be that high in cases where the company is proven to have deliberately violated the law.

Other jurisdictions globally do not appear to have acted to regulate consumer IoT as yet.

The benefit of analysing and benchmarking the situation in Europe and internationally has been that it has shed light on what are the non-regulatory and regulatory measures under consideration to address the problem of the cybersecurity of IoT devices. In terms of the findings:

- Both the EU and other jurisdictions globally are looking to introduce legislation to protect consumers using IoT devices.
- The relevant proposed and actual legislation from a RED perspective relates to device-level IoT security. However, there are also concerns about cybersecurity in enterprises and at the network level (botnet attacks using large numbers of unsecured IoT devices) and at the systems level (for instance, data protection and privacy in the transmission and storage of data in data centres); the latter, is outside the RED’s scope and covered by the GDPR.

4. Assessment of risks, vulnerabilities and consequences of breaches

This section provides an overview of the security vulnerabilities, risks and consequences of data breaches associated with different types of connected RE devices and wearables. It draws on a combination of desk research, interviews and product-based case studies.

4.1 Connected radio equipment – introductory assessment of risks and vulnerabilities

This section provides an overview of the vulnerabilities of different types of connected RE devices and wearables. It adheres to the conceptualisation of security breaches and their impacts presented in section **Error! Reference source not found.**. This separated the types of security breaches (physical penetration and online penetration) from the consequences that security breaches might permit (device fraud identity fraud and location breach).

This section reviews in more detail the different conceptual elements and provides examples of how the vulnerabilities and consequences can impinge on different application categories and different devices. Whilst the section provides insights to devices and consequences we believe the focus of revisions to a Directive must be on preventing the two main types of security breaches (physical penetration and online penetration). These vulnerabilities arise to different degrees across all relevant devices. If these can be addressed the adverse consequences of breaches will not arise.

Table 4.1 provides a broad overview of application categories in relation to different types of security breaches and consequences.

Table 4.1: Vulnerability of radio equipment to different security breaches and consequences

	Security breach		Consequence			
Application categories	Physical	Online	Device fraud	Identity fraud	Location breach	Devices 2030
Radio-frequency identification (RFID)			✓			53.8 bn.
Transport and traffic telematics	✓	✓	✓	✓	✓	132 m.
Smart home devices (alarms and telemetry)	✓	✓		✓	✓	4.5 bn.
Audio/media wireless streaming		✓		✓	✓	516 m.
Remote monitoring and wireless alarms	✓	✓			✓	387 m.
Wideband data transmission	✓	✓	✓	✓	✓	2.18 bn.

A short explanation of the allocation of application categories highlights that whilst the above table appears simple, it is subjective and there are both commonalities and differences in vulnerabilities between different categories of products. Considerations include:

- **Physical penetration:** All devices can be penetrated at some point in their lifetime. These devices can be penetrated 'in situ' during everyday operations;

- **Online penetration:** Nearly all devices transmit data (operational and sometimes concerning identity or location) via radio or fixed communications links. All devices, except RFIDs (which have no transmission capability) are therefore regarded as vulnerable by dint of being internet-connected. A direct internet connection is likely to be higher risk than an indirect connection, but the latter is not without risks;
- Consequences of device breaches will include:
- **Device fraud:** All radio devices could be liable to jamming or penetration with malicious intent. Those categorised in this group are particularly vulnerable to device fraud. Cloning has been reported for RFID chips and transport electronic fee collection devices and skimming have been reported for Near Field Communication (NFC) capabilities on smart phones, watches and other devices. These three application categories are therefore included in the above table;
- **Identity fraud:** Many devices require personal information to be provided by users during 'set-up'. Nearly all devices will be vulnerable to information loss and subsequent identity fraud during this initial registration process. This vulnerability therefore concerns radio devices that might transmit this data or other personal/organisational information more frequently. Some elements of this vulnerability are addressed by GDPR requirements for the collection and processing of personal data and by the privacy requirements for the transmission of electronic data via communications networks under the e-Privacy Directive. However, existing legislation covers legitimate use of data rather than deliberate attempts to misuse data for illicit purposes, such as identity fraud.
- **Location breach:** Like the previous consequence locational information is generally provided by a user during registration. This vulnerability therefore focuses on equipment that can be tracked to reveal the location of static and non-static radio devices. IP addresses associated with radio devices cannot generally be traced to a single address or post code area, but tracing to a city or region is usually possible.
- **Geolocational data breaches:** Many devices, such as mobile phones and smart watches, incorporate GPS and provide real-time information about the location of the user. An example is the widespread use of health app's to monitor people jogging / running. If accessed fraudulently, this could put the user in danger, especially children or other users that could be a target (e.g. military personnel).

It is evident that the consequences of a breach are largely dependent on the type and amount of information that a breach can 'expose'. Penetration wireless headphones or microphones will have few consequences, because they contain little information. Equally, penetration of a new laptop or tablet, containing no user or other 'sensitive' information, will also have limited consequences.

But when the laptop or tablet has been used for some time it could contain large amounts of information (such as personal detail, passwords and financial information) consequences could be considerable. This simple example highlights that the impact of focusing on devices or the consequences breaches can be spurious. Instead the Directive should focus on preventing the two main types of security breaches.

4.1.1 Stakeholder views and observations

It is clear from the targeted consultation that stakeholders believe that internet-connected RE devices create risks to data and privacy protection and protection from fraud, with 41% of respondents 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. However, several respondents indicated that the primary problem is not with the devices themselves but with the service providers.

Several interviewees acknowledged that whilst the scope of the RED applies to the connected radio equipment device or product, there are broader cybersecurity challenges relating to ensuring data protection and privacy and protection from fraud relating to **networks and IT systems as a whole, including data transmission to data centres and data centres where data is held**. A research paper on consumer IoT security with inputs from EU consumer associations points out in this regard that *"Existing product safety legislation and standards cover the safety of individual devices but may not be fit to properly protect consumers from the security risks of internet of things as devices are part of a bigger system."*[99]

A constraint however is that the RED can potentially address device related aspects of data protection, privacy and protection from fraud. It cannot directly prevent potential data breaches further up the data processing chain. However, security measures relating to passwords and encryption methods used by devices should ensure data security when it 'leaves' a device. Breaches in the data processing chain, beyond the device, are protected through the GDPR, with firms at risk of large fines if they do not protect customers' security adequately.

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, DVRs, and other IoT devices still using default passwords and then added them into a botnet network. This was then used to launch Distributed Denial of Service (DDoS) attacks on websites and Internet infrastructure, essentially making them unavailable. Although Botnets are outside study scope, since they are covered by Art. 3(3)d, 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 several stakeholders.

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[100] 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.

The two associations, supported by their national member associations therefore stressed the importance of ensuring that **security by design and default principles** are embedded into product lifecycle planning by manufacturers from the outset. They recommended that a **minimum set of security measures** should be obligatory for all connected RE products as a pre-condition for putting them on the market. These requirements should include *"at least encryption, software updates and strong authentication methods."* Moreover, it was suggested that "*the General Product Safety Directive as well as product specific safety legislation (Toy Safety Directive, Low Voltage Directive, Radio Equipment Directive, etc.) must be updated to ensure that they are in line with the new 'security for safety' concept of the general legal framework."*

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 therefore, also the data on a device or that the device is able to access (from other sources or devices). A number

[99] ANEC and BEUC. (2018). Cybersecurity for Connected Products: Position Paper. Ref: ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017. https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf.

[100] Cybersecurity for Connected Products, Position Paper, ANEC and BEUC, Ref: ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017, 7th March, 2018https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

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.

In previous literature, **shortcomings were identified from a security perspective** in respect of internet-connected radio equipment (RE) and wearables, especially in consumer IoT as these types of products are often cheap, lack sufficient security and are consequently easy to hack. A general lack of adequate security (including data protection and privacy and protection from fraud) in many consumer IoT devices and products has been noted in various literature (see bibliography in Annex 1).

The scale of the problem has grown in parallel with the increase in the manufacturing of such RE products and their usage in consumers' homes. A further trend is that products have become increasingly complex, as many electronic appliances commonly found in households (e.g. TVs, ovens, refrigerators, CCTV surveillance monitors) have transitioned from being unconnected, standalone devices, to being smart, connected and networked, either through an integrated Wi-Fi connection or indirect Bluetooth connection. Other consumer IoT products (e.g. tablets, wearables devices such as smart watches) have also become increasingly ubiquitous.

Many observers have pointed to evidence of inadequate security in IoT devices and smart products, varying from oversights in respect of the integration of minimum 'baseline' security requirements by design and default to the absence of any security considerations at all. Consumer IoT devices and smart product that are not secure may however still legally be on the European market if they are compliant with the core essential requirements set out in the RED, given that the various delegated acts relating to security aspects of products falling within the RED's scope have not been activated.

Despite the high level of consumer IoT devices that are inadequately secure, such products cannot presently be removed from the market if they are identified as posing unacceptable risks to security (and therefore safety) under existing EU legislation. The example of the Cayla doll scandal[101] demonstrated that existing EU industrial product legislation is insufficiently specific about the imperative of radio-equipped products being cybersecure to ensure high levels of consumer protection on the one hand and to help ensure a full and effective internal market in the area of radio equipment products. The presence of large numbers of legally-placed, but unsecure consumer IoT devices and products on the market could undermine the full and effective functioning of the internal market since currently, market surveillance and enforcement authorities are unable to remove such products, even if they identify them as being insecure and posing unacceptable risks (e.g., to children, data protection and privacy).

An example of the types of cybersecurity vulnerabilities associated with some consumer IoT products is provided in the following box, which focuses on internet-connected toys. This draws on research

[101] Myrstad, F. (2016). Connected toys violate European consumer law. https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/.

undertaken by the Norwegian Consumer Council, the findings from which have been presented at the G20 summit:

Box 4.1: Case study 1 - Security vulnerabilities in internet-connected toys

Product type: Connected toys

Cybersecurity vulnerabilities relating to data protection and privacy: the Norwegian Consumer Council carried out tests on internet-connected toys and identified a number of security vulnerabilities in products such as the Cayla doll. The Council looked into the technical features of selected connected toys, and the terms of use. The findings showed a lack of understanding of children's rights to privacy and security. Among the findings in terms of the vulnerabilities identified were that:

- The connected toy could engage in 'conversations' with children by using built-in microphones and speech recognition technologies. Spoken data, collected during the use of the toys, could potentially be shared with third-parties, especially via third-party mobile applications.
- There were identified risks from a child safeguarding perspective, since it was possible to use a mobile phone to speak to children through the toys using Bluetooth connections up to 20 metres away.
- The Bluetooth connection had not been secured, so the testing bodies were able to gain access without a password or other form of authentication.
- There were cybersecurity vulnerabilities in Cayla's software that allowed the doll to be hacked.
- A further problem identified was that marketing was found to be hidden, raising privacy concerns for children playing with the doll.

Whilst recognising some of the shortcomings identified, stakeholders from the toy manufacturers' industry contested some of the findings. For example, they pointed to the mention of commercial brands by the doll as being due to the manufacturer seeking to make the toy child-appealing and there was no intention of using hidden marketing.

Regulatory gaps: The Cayla doll example provides an illustration of regulatory gaps at EU level. Several flaws were identified in the product, which meant that it was not cyber-secure, and therefore exposed users to potential breaches of their data protection rights and did not adequately ensure their privacy. Despite this, market surveillance authorities (MSAs) were unable to remove the products under the RED or other EU legislation, since the Directive's essential requirements focus on: ensuring the physical safety of users using the product and on preventing harmful interference. Therefore, there was no scope to remove the Cayla doll, or similar products on the market under EU legislation. Nonetheless, some MSAs were able to remove the products using national legislation. But this meant finding creative ways of removing products from the market. For example, in Germany, a law preventing spying was used to ban such devices from recording children which was used to remove them from the market. Under the GDPR, whilst fines could have been issued against those unlawfully processing such data, this Regulation would not have allowed the products to be removed.

Impact of inadequate cybersecurity and identified vulnerabilities: Regarding the impacts, such products are often distributed widely and globally. For instance, Cayla and i-Que are distributed in the US, Norway, Sweden, Denmark, Australia, Netherlands, and the Middle East. They therefore pose an ongoing risk to children not only in Europe, but in other countries, and fail to protect children adequately. Overall, the Council found that the internet-connected toys My Friend Cayla and i-Que fail to safeguard basic consumer rights, security, and privacy. This was posited as being illegal since the report points out that "the right to privacy is enshrined in the European Convention of Human Rights, and further reflected in the European Data Protection Directive".

Industry feedback on how security concerns are being managed:

Recognising the complexity of the issues raised, it is important to provide an industry perspective and reaction to the issues raised both in relation to earlier security vulnerabilities in smart toys. The extent to which – and how – these are being addressed by industry but also to consider how large manufacturers of smart toys are embracing good practices to address the risk of vulnerabilities by designing these out from the outset of the design and engineering process.

Whilst recognising some flaws and vulnerabilities, toy manufacturers and their representatives noted that the industry is moving up the maturity curve and has made improvements over the development of successive generations of smart toys.

They also contested some of the findings from the research by consumer organisations. For example, the references to commercial brands among the phrases that the doll spoke were due to the manufacturer intending to use phrases and words the child may already be familiar with to make the toy appealing. There was no intention of using hidden marketing insofar as there were not commercial deals with place with the brands that were mentioned. The risks associated with Bluetooth connections were also seen as having been taken out of proportion in that the range of many Bluetooth devices is quite limited.

A further point raised was that whereas there has been a lot of media attention to concerns regarding data getting into the wrong hands, the fears may be overblown. Non-sensitive personal data tends to be gathered by many smart toy products partly due to the strict regulatory regime under which global manufacturers have to operate (e.g. GDPR in Europe, COPPA in the US) regarding data collection and processing. This means that the impact of a hacking attack could be localised to the relatively limited data collected on the device itself.

The large toy manufacturer interviewed explained that they already treat children's data protection and privacy seriously and have integrated security by design and default principles into their business processes. This has complemented more specific procedures relating to data protection and privacy by design and default required under EU legislation (e.g. the GDPR and e-PD) in the design of smart toys.

Large manufacturers are concerned about such issues both due to non-regulatory and regulatory drivers. From a non-regulatory perspective, leading toy manufacturers recognise that their main customer base is children and young people and are therefore concerned about the potential reputational issues if they did not take such issues very seriously and integrate them into business processes. Moreover, it was pointed out that smart toys are an increasingly regulated market, and therefore have to be designed accordingly, with a consequent reluctance among some leading manufacturers to collect any more than the absolute minimum personal data and information when the product is registered. In Europe, the GDPR has made a significant difference in that business processes have to be more carefully documented to demonstrate that data protection and privacy by design and default (and appropriate technical and organisational measures) have been implemented during the design and engineering phases, supported by extensive testing.

In the US, there is already longstanding legislation through the Children's Online Privacy Protection Act (COPPA), a U.S. federal law which took effect in April 2000 designed to limit the collection and use of personal information about children by the operators of Internet services and Web sites. A further risk for manufacturers is that other actors in the value chain may take decisions outside their control regarding selling particular smart toys if they perceive that the toy concerned does not meet particular requirements. "Stores may make decisions based on their interpretation of the law". Therefore, big manufacturers increasingly tend to play it very safe by avoiding taking risks with product security, reducing the amount of personal data that they collect and transmit via internet and containing much of the data on the localised device.

Source: CSES analysis based on interview and desk research to review the Toy Fail[102] report by the Norwegian Consumer Council[103]

[102] Myrstad, F. (2016). #Toyfail - an analysis of consumer and privacy issues in three internet-connected toy - https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf

[103] Myrstad, F. (2016). Connected toys violate European consumer law. https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

It should be noted that as the issues are complex, reference should be made to the full-length case study on smart toys.

Such vulnerabilities are not confined however to internet-connected smart toys.[104] Research by BEUC[105] into the security of consumer Internet of Things (IoT) devices more generally points to a number of basic security flaws in many products and devices, such as the **use of unprotected, default passwords** and **risks from connecting multiple IoT devices to home networks** if either one or more of the devices themselves, or the wireless router does not have appropriate security protection. *"In many jurisdictions, existing product safety legislation and standards cover the safety of individual devices but may not be fit to properly protect consumers from the security risks of internet of things as devices are part of a bigger system. To ensure the safety of the system as a whole, additional provisions and standards will need to be adopted when the device is controlled and operated as part of a wider IoT system" (page 3).*

4.2 Synthesis assessment of security vulnerabilities and technical solutions in internet connected radio equipment products

This section contains a synthesis assessment of security vulnerabilities identified through the IA study. It draws on the findings from the six product-based case studies (covering laptops, routers, security cameras and baby monitors, Smart Toys, Smart TVs and Smart Watches), presented as a standalone annex. In addition, material from a lawnmowers case study in this report is provided. Furthermore, the analysis considers interview feedback and the findings from the desk research relating to potential security vulnerabilities – and technical solutions to mitigate these - associated with additional different types of connected RE products, for instance, smart alarm systems, smart meters and mobile phones. Whilst using insights from different types of devices to illustrate a variety of impacts it must again be emphasised that most vulnerabilities (related to physical penetration and online penetration breaches arise to different degrees across nearly all devices.

4.2.1 Security vulnerabilities in internet-connected RE products

The case study research has identified security vulnerabilities in respect of connected RE, especially in consumer IoT devices directly connected to the internet. Among the issues highlighted were:

- Predominantly similarities and few differences in respect of the different types of security vulnerabilities across different categories of internet-connected RE products.
- Differences in the nature and extent of security vulnerabilities – and the impacts of these materialising - between 'simple' and more 'complex' internet-connected RE products.

The remainder of this section provides examples of vulnerabilities, breaches, loopholes and risks. Simple radio equipment covers internet-connected RE devices that have one, or only a small number of core functions, such as wireless cameras, routers, baby monitors, connected toys, etc. as opposed to "complex equipment" e.g. laptops and smartphones that may collect many different types of personal data on the hardware, software and chips.

4.2.1.1 Similarities and differences in security vulnerabilities across internet-connected RE products

The key findings were that:

- Some security vulnerabilities are applicable across all categories of internet-connected Radio Equipment products, due to their dependence on wireless internet and network communications

[104] Maras M.-H. (2015). The Internet of Things: Security and Privacy Implications. *International Data Privacy Law*, *5*(2), 99–104.

[105] ANEC, BEUC, Consumers International, and ICRT. (2017). Securing consumer trust in the internet of things: Principles and Recommendations. https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf.

technologies and vulnerabilities in wireless internet security protocols.

  - The wide prevalence of WLANs means that data may be at risk of being compromised as flaws have been discovered in security protocols that are part of the 802.11 wireless LAN standard necessitating these protocols to be updated and strengthened progressively over time.
  - There have been a number of new vulnerabilities identified in relation to WLAN security protocols that could lead to data breach problems, which would result not only in data protection and privacy breaches, but also expose users to fraud.
  - However, as with any technology, new security vulnerabilities are regularly identified, and these are addressed by the IEEE, working in close conjunction with industry. Once security vulnerabilities are in the public domain, industry and international standards organisations work to address these over successive generations of the development of wireless standards, which include a strong focus on improving security protocols.

- Regarding simple and complex internet connected radio equipment, this is a rather arbitrary distinction from a security vulnerabilities and risk perspective. It is quite difficult to categorise and define precisely what is meant by a 'simple' as opposed to a 'complex' RE product, as there could well be a blurring of the delineation between the two. Fundamentally, if a device is internet-connected, it can be hacked irrespective of whether it is simple or complex.
  - Whilst complex devices, such as laptops and smart phones, collect multiple types of data via a combination of chips embedded in the hardware and software, simple devices also collect and transmit person data using a combination of hardware and software, and could similarly be hacked.
  - Complex devices have greater functionality and the broader this functionality, the more likely it is that there will be more EO in the value chain. There is therefore a multiplicity of risks in terms of access points to data.
  - However, there could be some aspects of complex devices where some degree of differentiation in terms of risk levels can be discerned. For instance, laptops and smart phones have many different types of software and applications loaded on them at placing on the market stage (and especially so once the user starts to download additional app's), compared with simple products.
  - Therefore, the greater the number of third parties involved, the higher the risk of one of these pieces of software or app's being hacked or penetrated. Balanced against this, more complex products, such as laptops and smart phones, are part of huge industries selling in significant volume and with a longer history of implementing security on their devices. Therefore, such manufacturers have higher levels of maturity in terms of investing in security solutions compared with simple and newer smart devices, especially those produced in lower quantity. As such, it is very difficult to generalise about the level of vulnerabilities, risks and impacts associated with simple vs. complex products.
- The product case studies showed that several other types of security vulnerabilities are common across product groups, with the risks primarily being due to the radio device being internet-connected, rather than the specific characteristics of the product itself. A further commonality is that at the cheaper end of the market, some producers provide low-quality connected RE products that may not be on the European market for that long, but which lack minimum basic security functionality. For instance, such products may be non-password protected, not require authentication and use cheap chips without either adequate, or in some cases any consideration given to basic encryption to protect users' data either on the device itself or in the transmission of data from the device. This does however depend greatly on the type of product and price point.
- However, other types of security vulnerabilities identified were found to be specific to the product

type in question. For example:

- A particular problem with **Smart TVs** is that firmware and software are often not maintained beyond a couple of years following placing on the market. Whilst outside the RED's scope (concerned with checking compliance with the essential requirements pre-market access), this could nevertheless pose risks in terms of the risk of data breaches for other types of internet-connected RE devices unless these have adequate security, and the internet traffic could then be intercepted, either passively or aggressively by a third party.
- The security vulnerabilities for **routers** on the one hand tend to relate to the lack of basic security by design and default functionality (but among low-priced, low-quality products only as other manufacturers take security very seriously) but on the other to more complex risks, such as the risk of TCP injections and of third parties trying to mimic the router and thereby expose the user to malicious code or malware.
- Regarding **laptops**, statistics show that laptops (and other complex products such as mobile phones) are among the connected RE products where instances of data breaches, hacking, malware penetration of the device etc. are most common. However, the nature of security vulnerabilities and risks is complex, ranging from the manufacturer's hardware, to third party software and app's that users have themselves downloaded to the laptop or mobile phone device post market-placement. Whilst users' data and privacy are protected by the responsibilities of the data controller (and data processors in their supply chain) by the GDPR, this relates to responsible and traceable economic operators only. There are often other security vulnerabilities that could compromise the device and lead to a data breach due to malevolent intentions on the part of hackers, malware designers etc. that could risk data being compromised. One of the security-related problems for laptops at a lower price level is that they are much less likely to use encrypted chips and therefore, data may be unencrypted.
- Turning to **security cameras and baby monitors,** unless these are properly secured, they raise considerable privacy concerns. The most common problems in relation to CCTV cameras ad baby monitors were found to relate to the use of default passwords, which many users fail to change. However, there are also other exploitable problems with IP security cameras. For instance, IP cameras were attacked for instance through the Mirai botnet in 2016[106], a DDoS attack which shut down many leading internet sites. Although DDoS attacks affecting many thousands of devices will be the subject of a separate study, it illustrates that individual connected RE devices remain vulnerable. However, some of the risks associated with hacking of IP cameras are not fundamentally different from the privacy considerations associated with using other smart devices embedding a camera (such as mobile phones[107]). The difference is that hacks involving IP cameras attract a lot of media attention, for instance due to concerns about children's safety.
- Some **robot vacuums also contain cameras**, and these have been found to have poor security. However, some research has shown that **communication security of the local data connections between the robot and the app via Wi-Fi** (i.e. the local area network) posed limited risks, as data transmission occurs between the app and the robot in a limited space in home Wi-Fi ranges. Attackers would therefore have to be physically located in the immediate vicinity in the transmission range of either the robot vacuum or the router to be able to access data.
- Regarding **smart watches,** among the main security vulnerabilities identified were: the risk of exposure of confidential geo-locational data, especially for vulnerable users, such as children.

[106] Among the many articles focusing on the vulnerabilities of IP cameras - https://www.iotworldtoday.com/2019/08/31/5-cybersecurity-lessons-related-to-ip-security-cameras/

[107] There is an app to access both of the phone's cameras.

As many smart watches are aimed at children, this is a concern. Among the findings of a piece of research from 2017 [108] on smart watch vulnerabilities was that there was little awareness regarding privacy and security issues for smart watches, either among manufacturers or consumers. One of the further concerns wearables such as smart watches is that they collect, produce and communicate a wide variety of data ranging from structured data (e.g. number of steps taken, distance travelled, speed and pace, calories burnt, heart rate, skin temperature, perspiration level, hours slept, to dietary information to unstructured voice and video recordings.

- As regards **alarm systems,** it was stressed that the extent and nature of vulnerabilities varies depending how - and whether – alarms are smart, and if yes, whether these are connected directly or indirectly to the internet.
- Statistics suggest that whilst **communication technologies through mobile internet** are generally secure (in terms of the security of the network), there are device-level vulnerabilities associated with mobile phones, often stemming from the third-party app's and software downloaded onto the device by users, as well as a result of external communications received onto the device, which may have malware embedded).

An example of the challenges in addressing device-level vulnerabilities in mobiles is now provided. It should be stressed that whilst the mobile phone industry when interviewed highlighted that the industry is mature in addressing security vulnerabilities, the research suggests that whilst this is true at the network level, devices may be penetrated due to their interaction with other app's, software and malware. Indeed, personal data theft via laptops and mobile phones are among the most commonly reported sources of data breaches and theft.

Box 4.2: Mobile phone hacking via third party app's

There are several ways in which WhatsApp can be hacked, even though messages are end-to-end encrypted by default. This includes three examples of hacking risks, which have now been patched and two examples of risks of privacy being compromised and of social engineering to gain access to data to commit fraudulent activity, such as theft and identify fraud.

1. Remote Code Execution via GIF. The hack works by taking advantage of the way that WhatsApp processes images when the user opens the Gallery view to send a media file. When this happens, the app parses the GIF in order to show a preview of the file. GIF files are special because they have multiple encoded frames. This means that code can be hidden within the image. If a hacker were to send a malicious GIF to a user, they could compromise the user's entire chat history.

2. Pegasus Voice Call Attack. Allowed hackers to access a device simply by placing a WhatsApp voice call to their target. Even if the target didn't answer the call, the attack may still be effective. The target may not even be aware that malware has been installed on their device. This has been used in state-sponsored hacking in well-publicised cases.

3. Media File Jacking - takes advantage of way that apps receive media files like photos or videos and write files to a device's external storage. The attack starts by installing a malicious piece of malware hidden inside an apparently harmless app. This malware can then monitor incoming files for Telegram or WhatsApp. When a new file comes in, the malware can swap out the real file for a fake file.

4. Facebook – risk of the owner of WhatsApp being able to read WhatsApp chats. Although the company makes clear that it does not read WhatsApp messages as they are end-to-end encrypted not all messages are fully private. On operating systems such as iOS 8 and above, apps can access files in a "shared container." Both Facebook and WhatsApp use the same shared container on devices. While chats are encrypted when they are sent, they are not necessarily encrypted on the originating device.

[108] Popescul, Daniela & Georgescu, Mircea. (2017). A User Perspective on the Vulnerabilities of Smart Watches: Is Security a Concern?. Timisoara Journal of Economics and Business. 10. 135-150. 10.1515/tjeb-2017-0009.

This means the Facebook app could potentially copy information from the WhatsApp app. There is no evidence that Facebook has used shared containers to view private WhatsApp messages. But the potential ability is there for them to do so.

5. Not all security vulnerabilities are technological – risk of social engineering. Social engineering, a concept in which human psychology is exploited to steal information or spread misinformation. An example of a risk was identified by security researchers which allowed people to misuse the quote feature in group chat to alter the text of another person's reply by decrypting WhatsApp communications, which allowed them to see data sent between the mobile and web versions of WhatsApp. They could change the values in group chats and impersonate other people, sending messages which appeared to be from them. They could also change the text of replies. Such scams and faking communications data so that it appears real and cons people into providing data is not unique to mobile phone app's as there have been many similar scams attempted via conventional voice calls and SMS.

It should be stressed that several of the above vulnerabilities have now been (security) patched via software updates. Nonetheless, they are useful in illustrating the complex inter-play between device-level security and the security of individual pieces of software and app's, be they downloaded onto the device by users or pre-loaded as part of a package when the device is placed on the market. n

Source: Makeuseof.com https://www.makeuseof.com/tag/how-whatsapp-messages-can-hacked/ , editing by CSES.

The purpose of the above example is to demonstrate that as mobile phones contain extensive personal data both on the device, and within app's, they are a major target for data theft. However, a problem from a regulatory perspective is that such security vulnerabilities only fall under the RED's Article 3(3)(e) and 3(3)(f) and if the device might have preloaded software and third-party app's prior to placement on the market. However, if Article 3(e)(i) were also to be activated (software), then the manufacturer would be under responsibility to check that third-party software did not compromise the device's security and lead to a potential data breach.

Therefore, the RED could still play a role in requiring manufacturers to reflect on how the device interacts with third-party apps. For example, videos and images may be automatically saved to the device's folders by default, meaning that an infected piece of malware would then be on the device, not only the app, which appears to be a security gap. The complexity of the value chain for a ubiquitous device such as a mobile phone therefore needs to be taken into account. This implies that only in activating several of the delegated acts such as Article 3(3)(d), Article 3(3)(e), Article 3(3)(f) and Article 3(3)(i) could a value-chain wide approach be ensured to preventing device-level compromising attacks leading to data breaches.

4.2.1.2 Common risks linked to Wi-Fi and LAN internet-connections

802.11 Wireless Local Area Networks (LAN's) have become one of the main access points to internet networks. The 802.11 standard has evolved since its launch in 1999. For example, in the past five years, higher-speed standards such as the 802.11n and 802.11p have been developed. Wi-Fi has replaced the Ethernet as the main method of network access, driven by the proliferation of internet-connected RE devices. More portable devices, especially mobiles and laptops, but also other products have led to a significant need for WLAN in home networks and in other locations such as coffee shops, educational institutions, airports, offices, government buildings, etc.

Although there have been improvements over successive generations of development of such technologies, equally security vulnerabilities have been identified progressively in new generations of Wi-Fi, which have in turn required further re-engineering and the launch of Wi-Fi with improved security.

Wireless local area network (WLAN) provides a direct internet connection for many different types of internet-connected radio equipment. Widely adopted standards such as IEEE 802.11, commonly referred to as Wi-Fi, have been integrated into tens of millions of wireless connected RE devices. The standards used in such technologies have been developed by international standards bodies working in close conjunction with industry, namely the Institute of Electrical and Electronics Engineers (IEEE), and the LAN/MAN Standards Committee (IEEE 802). The standards have been updated as successive generations of Wi-Fi technologies have been developed, commencing with IEEE 802.11a and b in 1997 through to 802.11p. The IEEE 802.11 standard provides two modes of authentication: open system authentication and shared key authentication. It also incorporates different encryption technologies, which have evolved over time as security vulnerabilities have been identified.

Incremental improvements in security protocols for wireless networks have been made over time as new security vulnerabilities have been identified. [109]Overall, wireless networks remain very popular as a convenient way of connecting to the internet, but there are **security issues compared with traditional wired connectivity**. [110]As wireless networks use electromagnetic waves to transfer data, it is easier for third party users to gain access to the data being transferred between a client and access point. This demands a combination of security features, such as encrypted authentication and data transfer; and extra security layers such as a firewall and intrusion detection/prevention systems. To meet this challenge, there has been an evolution in security protocols and encryption methods since the late 1990s until today, as shown in the box below:

Box 4.3: Evolution in wireless security protocols (including encryption and authentication technologies)

The wireless standard 802.11 Security Architecture has evolved over time since the launch of WEP in 1999. A summary is provided below.

- **WEP (Wired Equivalent Protocol) -** launched in 1999 as the earliest wireless protocol. The goal was to prevent eavesdropping on network traffic. Whilst WEP was meant to provide the same level of security to wireless networks as wired, it was discovered that the 40-bit encryption key was easily hackable. WEP is today seen as weak and outdated.
- **WPA -** was a stronger encryption method, in which data dynamically changes using a stronger encryption method, **TKIP (temporal key integrity protocol).** The WPA protocol increases security by introducing two new protocols: a four-way handshake[111], and the group key handshake. Although a major improvement on predecessors, a risk of data breaches was identified.
- **WPA2** uses **AES (advanced encryption standard)**[112] and was considered the most secure method of protecting Wi-Fi connections in 2004, when launched. However, some security researchers believe that WPA2 is not significantly more secure than WEP itself (see Schenk, Garcia and Iwanchuk, page 16).
- **WPA3** – launched in 2018. Cutting-edge security protocols, with increased protection from password-guessing attempts.

[109] See for example https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/ and WiFi (Wireless) Password Security - WEP, WPA, WPA2, WPS Explained, Apr 26, 2019, https://www.youtube.com/watch?v=WZaIfyvERcA

[110] Wireless LAN Security Threats & Vulnerabilities: A Literature Review, Md. Waliullah and Diane Gan, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014

[111] The four-way handshake is an authentication process that occurs between an access point and the client.

[112] Advanced Encryption Standard (AES) is a block cipher. With chunks of data encrypted at once, data is diffused within the block after encryption, rather than being allocated in a linear fashion.

Some security vulnerabilities have been identified relating to Wi-Fi technologies by security researchers. This often involves the identification of a vulnerability that could theoretically be exploited rather than result from an actual hack. Nevertheless, when such flaws are identified, they require being designed out as part of the process of the incremental development of successive generations of wireless internet security protocols. For instance, in the case of WEP, WPA and WPA2 and WPA3, security vulnerabilities were identified, which have necessitated work to rethink some security aspects of the security protocol and standard.

Box 4.4: Weaknesses in the WPA2 protocol

Weaknesses in the WPA2 protocol were identified by security researchers from Louvain University. WPA secures many protected Wi-Fi networks. According to the researchers, an attacker within the range of a target victim could exploit weaknesses using **key reinstallation attacks (KRACKs)**. Attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This could lead to sensitive information being stolen such as credit card numbers, passwords, chat messages, emails, photos, etc. The attack works against all modern protected Wi-Fi networks. Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites.

The weaknesses are in the Wi-Fi standard itself, and not in individual products. Therefore, any implementation of WPA2 is likely affected. To prevent the attack, users must update the affected products as soon as security updates become available.

Source: Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 presented at the Computer and Communications Security (CCS) conference, Mathy Vanhoef and Frank Piessens, Wednesday 1 November 2017. https://www.krackattacks.com/

The development of new technologies and new market sectors such as connected cars embedding multiple sensors which collect and transmit real-time data means that there is a need to develop next generation wireless technologies able to accommodate new development, whilst at the same time improving security. For example, the IEEE 802.11 Next Generation V2X (NGV) Study Group is exploring ways to leverage more recent 802.11 technologies to address new applications of wireless access in vehicular environments, where new requirements for higher throughput, improved reliability and efficiency, and/or extended range are anticipated[113]. Whilst such protocols are developed with security closely in mind by design and default, new security vulnerabilities may be identified in future. The lesson learned is that if the delegated acts were to be activated in the fields of data protection and privacy and protection from fraud, there would be a need to keep standards under review, and to recognise that new security vulnerabilities are regularly identified, requiring the ESOs to monitor and update technical standards, and industry to update the standards they comply with accordingly. It should be stressed that this process is already happening anyway among many leading industry players, and it is therefore more a question of ensuring that all EO do so than imposing many new requirements (if existing standards were to be used as the foundation – see section on technical solutions and mapping by the ESOs of available standards).

Indirect connections are commonly used in internet-connected RE devices, such as connecting devices using short-range communication protocols such as Bluetooth, a 2.4 GHz personal area network for short-range wireless communication. [114]. There are other examples, such as ZigBee, a 2.4 GHz mesh local area network (LAN) protocol, Z-Wave is a sub-GHz mesh network protocol often used for security

[113] https://standards.ieee.org/news/2018/ieee_802-11_study_groups.html

[114] Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances. Bluetooth is used to connect short-range devices such as mobile phones, computers and peripherals to transmit data or voice wirelessly over a short distance.

systems, home automation and lighting controls and 6LoWPAN uses a lightweight IP-based communication to travel over lower data rate networks.

All kinds of RE devices can be indirectly connected to the internet, such as **keyboards, mice** and **speakers.** A key difference between using a LAN is that smaller devices can be indirectly connected to the internet as the direct internet connection is provided using a Wi-Fi connection via a router or a LAN or Wi-Fi connection via a mobile phone.

In terms of the level of security risks that indirect internet connections pose, these represent a lower risk for various reasons, such as any attempted hacker needing to be within the local physical range of the Bluetooth or other type of connected device using radio frequency communications, which may be constrained to as little as 10-20m before the signal is lost. However, this is not to suggest that devices indirectly connected to the internet are not at risk, as Bluetooth-connected devices are also at risk of being hacked. Moreover, the latest generation of Bluetooth technologies has greater range and devices can be connected in some cases up to 250-300m away. The security vulnerabilities associated with such communications technologies are broadly similar irrespective of the connected RE product.. A key problem, noted several times previously, is that users must set a password to allow a devices to communicate and share data. But users often fail to reset the default password and as consequence data communicated from the device is left largely unsecured enabling anyone that knows the default password to access it. This common problem could be addressed if manufacturers ensured that 'set-up' procedures for a new device make it mandatory for users to select a new password.

A challenge in differentiating the level of risk for regulatory purposes is that many connected RE products include both a Wi-Fi connection and Bluetooth or other communications protocol to allow wireless data sharing. Therefore, it would be difficult to regulate only Wi-Fi products, but not Bluetooth products in many cases as there is both LAN and Wi-Fi connectivity. There are however also examples of products that either have a wireless connection or Bluetooth connectivity but not both. Examples from the product case studies (see standalone annex) are the security cameras and baby monitors market, which are differentiated between products that are IP-enabled with direct access to the internet, products with localised connectivity, for example through Bluetooth and products that cannot be internet-connected at all, which instead use low-medium range radio frequency. The latter eliminate the risk of security vulnerabilities linked to being connected altogether, although radio frequencies can be hacked, but are out of scope of the RED as there is no radio device integrated.

It is therefore be possible to differentiate between the level of risks associated with directly internet-connected baby monitors, which pose the greatest risk as they can be hacked from anywhere in the world, whereas hacking an IP-based baby monitor (or a security camera) would require a more localised physical presence, as it is only connected indirectly to the net. A particular area of risk is that some baby monitors and security cameras record video and sometimes sound and this is saved and backed-up in the cloud. Any such product where there is cloud-based personal data being retained means that there are additional risks, however, these are communications network-related risks of data breaches and covered by both GDPR and the e-Privacy Directive. As the RED is concerned with the product pre-placement on the market, cloud-based data related vulnerabilities fall outside the Directive's scope but perhaps highlight the importance of looking over the medium to longer term at how industrial product and data protection and privacy legislation might protect user security holistically, from the device itself (falling under the RED) through to the data transmitted electronically and secured on the cloud in a data centre (falling under the GDPR and the e-Privacy Directive).

4.2.1.3 Privacy considerations – loopholes in terms of how connected RE devices use and exploit data collected

There are privacy considerations concerning the types of personal data and non-personal technical information (for example, about product performance) is collected by internet-connected RE devices, and how such data is used by manufacturers, technology and service providers.

Taking security cameras as an example, whilst the GDPR protects users in the processing of their data (or in the case of security cameras, their video footage), users of security cameras may not be aware that when agreeing to the terms and conditions, they may inadvertently have allowed significant amounts of their personal data to be resold and exploited for commercial purposes. An example of a well-known manufacturer of security cameras was identified for instance where both the manufacturer and its ultimate owner, an e-retailer (and any of its licensees) held "an unlimited," "irrevocable," "perpetual" and "worldwide right to reuse, distribute, store, delete, translate, copy, modify, display, sell" video footage.

The company's terms of service also give the company concerned the authority to "create derivative works" from footage "for any purpose and in any media formats in any media channels without compensation to you." This raises privacy concerns as to whether there is an appropriate legal basis for such processing. Arguably, reminding economic operators of their obligations in their capacity as either data controllers or processors under the GDPR by activating the delegated act on data protection and privacy (i.e. Art. 3(3)(e)) could serve to reinforce GDPR implementation.

This raises issues relating to GDPR implementation from a connected RE device users' perspective such as on the extent to which users are aware of the different types of processing carried out with their data and to what they are consenting too, . GDPR consent requires specific and separate consent, which must be distinct from the T&C outlined in the contract. The change of T&C in itself does not provide a legal basis for processing as there must be an appropriate data protection notice, and appropriate consent obtained where needed. If processing changes, new consent must be sought.

4.2.2 Analysis of security vulnerabilities by product, risk assessment and degree of impacts

The previous section provided 'real world' insights to the security breaches and consequences used in the conceptualisation used to underpinning this study; first presented in section **Error! Reference source not found.**. The vulnerabilities of different devices were used to illustrate the variety of ways in which the two common flaws in devices (physical penetration and online penetration) can arise.

This section reviews in more detail the different conceptual elements and provides examples of how the vulnerabilities and consequences can impinge on different devices and device categories. **Error! Reference source not found.** provides a broad overview of devices and device categories for the two types of security breaches and the three types of consequences.

The comparison across devices categories presented in **Error! Reference source not found.** should be treated with caution. It includes generalisations about devices and the subjective views of our team about the extent of vulnerabilities and consequences. For example, the preceding section highlighted that there are differences in the functionality and operations of devices within the same category (for example the functionality of different types of baby monitoring devices), further details are provided in the next sub-section.

Nonetheless, **Error! Reference source not found.** provides some insights to the relative vulnerability of devices and the magnitude of consequences. The analysis presented in the table also provides insights to the common features that affect scores.

The columns with the red header provide an assessment or score for the level of vulnerability of devices for the two main types of breaches - A score of five indicates high vulnerability, zero indicates no vulnerability.

The degree of risk for physical penetration (red column A) is largely related to the location(s) of a device. A device located in a building (home, workplace or other) is generally regarded as relatively secure and is allocated a score of 2 or lower. Physical penetration of a device would require the perpetrator to access the building and then to access the device (either in-situ or subsequently after the item had been stolen). A slightly higher score of 3 is allocated to devices that might generally be used in a building but occasionally might be used elsewhere (e.g. warless headphones, laptops or tablets). Highest physical vulnerability scores of 4 or higher are allocated to devices that are generally used or located outside buildings, these include autonomous vehicles and telemetry equipment.

The degree of risk for online penetration (red column B) is largely related to the nature and extent of communications. Communication over short distances (approximately 10 metres), generally facilitated by Bluetooth, is regarded as a relatively low risk (scoring 2 or lower). Mobile communications over a wider area (via a SIM card or internet) is regarded as more vulnerable to online penetration are scored more highly (3 or above).

Although under-pinned by the preceding 'logic' the scoring system is subjective and even for the same device type differences might occur due to the different functionality of devices.

The orange headed columns are added to provide insights to the three mains consequences of a breach. Once again scores are provided in the range 1 to 5. For all three consequences (device fraud, identity fraud and location breach) the score is mainly founded on the amount and the sensitivity of information that someone penetrating a device will be able to access. As repeated several times previously – the consequences of a breach can be disruptive or far worse. Whilst consequences might be significant the focus of amendments to the Directive must be on devices. Most notably preventing physical penetration and online penetration. If penetration can be averted consequences might be minimised or prevented entirely.

Table 4.2: Cross-comparative summary of security vulnerabilities of radio equipment

Device type	Data shared at workshop	Estimate EU28 2015	Forecast EU28 2020	Forecast EU28 2025	Forecast EU28 2030	A Physical penetration Risk	B Online penetration Risk	Total	C Device fraud consequence	D identity fraud consequence	E Location breach consequence	Total
1 ACTIVE MEDICAL IMPLANTS												
a Implantable cardiac pacemakers, ICDs & CRTs	Yes	4.46m	4.48m	4.52m	4.54m	0	2	2	0	0	0	0
b Cochlear implants	Yes	87,900	167,500	322,500	621,000	1	2	3	0	0	0	0
2 RFID												
a Passive	Yes	3.7bn	24.7bn	40.5bn	66.4bn	1	0	1	0	0	1	1
b Active	Yes	37m	247m	405m	664m	1	3	4	3	2	2	7
3 TRANSPORT AND TRAFFIC TELEMATICS												
a Embedded vehicle anti-collision radar	Yes; S cars	3m	11.82m	45.2m	132m	5	4	9	5	5	5	15
b Electronic fee collection	Yes; S cars	31,290	31,290	31,290	31,290	4	0	4	4	4	4	12
4 ALARMS, TELECOMMAND AND TELEMETRY												
a Wireless alarms	Yes, S homes	Smart home devices 210m	Smart home devices 850m	Smart home devices 2.95bn	Smart home devices 4.5bn	2	2	4	4	5	1	10
b Key fobs	Yes, S homes					2	0	2	4	3	1	8
c Baby Monitors	Yes, S homes					2	3	5	2	3	1	6
d Garage door/gate openers	Yes, S homes					2	0	2	3	4	1	8
e Telemetry equipment	Yes, S homes					4	4	8	4	4	2	10
f Telecommand devices	Yes, S homes					2	3	5	4	4	2	10
5 AUDIO/MEDIA WIRELESS STREAMING												
a Wireless headphones	Yes	14.1m	38m	47m	48m	2	0	2	1	2	1	4
b Media players	Yes	55m	196m	243m	250m	2	0	2	1	2	1	4
c Wireless Speakers	Yes	5.2m	36m	104m	150m	2	0	2	1	2	1	4

Device type	Data shared at workshop	Estimate EU28 2015	Forecast EU28 2020	Forecast EU28 2025	Forecast EU28 2030	A Physical penetration Risk	B Online penetration Risk	Total	C Device fraud consequence	D identity fraud consequence	E Location breach consequence	Total
d Wireless microphones	Yes	1.5m	10 - 15m	50 - 70m		2	0	2	1	2	1	4
6 REMOTE MONITORING AND WIRELESS ALARMS												
a Water, electricity, gas meters	Yes	54.1m	250 - 275m	635 - 660m		2	2	4	2	2	1	5
b Social alarms	Yes	2.6m	4.2m	4.9m	5.2m	2	0	2	1	2	1	4
c Distress alarms	Yes	2.7m	6.7m	8.7m	10m	2	0	2	1	2	1	4
7 WIDEBAND DATA TRANSMISSION												
a Laptops with wifi	Yes	404m	371m	250m	101m	3	3	6	4	4	2	10
b Tablets	Yes	120m	299m	404m	440m	3	3	6	4	4	2	10
c Public access points	Yes	803,000	2m	6.8m	14m	3	3	6	5	5	1	11
d Smartphones	Yes	566m	807m	824m	824m	3	3	6	4	4	2	10
e Games consoles	Yes	27m	62.2m	75.1m	77.4m	2	3	5	3	2	2	7
f Smart Televisions	Yes	17m	45m	137m	227m	3	3	6	4	4	2	10
g Wearable devices	Yes	8.5m	102m	388m	567m	2	3	5	3	2	2	7
h Virtual reality head display	Yes	1m	17m	65m	78m	2	3	5	3	2	2	7

Source: Tech4i2 analysis

Key:

A Physical penetration risk	Considers the likelihood of physical security penetration and/or external port access to or from a device.
B Online penetration risk	Considers the likelihood of unauthorised digital access to a device or network communications
C Device fraud consequences	Considers the magnitude of impact of mischievous and/or malicious use (malware or remote access), device cloning and unauthorised use of digital signatures
D Identity fraud consequences	Considers the magnitude of impact of unauthorised access to personal and organisation information
E Location breach consequences	Considers the magnitude of impact of unauthorised access to location information.

The key provides an explanation of the different types of penetration risks, and of the consequences of data breaches occurring, focusing on device fraud, identify fraud and location breaches.

Error! Reference source not found. highlights that no device is hugely more vulnerable than other device. It is obvious that devices 'outside' in public places are more vulnerable to a physical breach than those 'inside' generally used in buildings. It is equally obvious that short range connectivity via Bluetooth or similar communications is less likely be penetrated than communications that might be transmitted globally via the internet. Selecting any particular device for attention in updates to the Directive therefore makes little sense.

The table shows that the two main vulnerabilities (physical penetration and online penetration breaches) arise to different degrees across all relevant devices. If these two can be addressed the unpleasant consequences of breaches will be diminished or prevented. We therefore suggest that addressing these two vulnerabilities across all devices is the most obvious focus for updates to the Directive. A focus on any single device or small number of devices will undoubtedly develop recommendations or requirements that will be relevant to nearly all other devices.Market dynamics and the implications for security vulnerabilities

To further emphasise differences between devices of the same type this section provides a short overview of handful of devices and devices with different characteristics. These differences also emphasis complexities that might have to be addressed if amendments to the Directive were to focus on particular devices

Preceding sections have demonstrated that some devices are at greater risk of physical and online penetration than others and the complex nature of comparisons between products. For example, a product may be higher-risk, but steps could already be being taken by the industry to address the security vulnerabilities identified, either through the development of technical standards, or by 'designing out' security vulnerabilities from the outset. This also depends on the level of maturity of a particular sub-sector and the level of investment the industry is able to make. The amount of security vulnerabilities is not fixed, but changes over time, depending on the product, how proactive manufacturers are in a particular sub-sector in addressing security vulnerabilities, and the suitability of specific technical solutions to address these vulnerabilities.

For example, in the case of **smart toys,** the case study showed that although there have been a number of incidents relating to poor security of such internet-connected products, raising concerns about children using the products, it was pointed out that the industry is dominated by a small number of big market players who are strongly aware of the problem, and associated reputational issues if they do not integrate sufficient security into products. Evidence was identified of progress over successive generations of smart toys in designing out potential security vulnerabilities. In other words, there is a level of maturity among the main industry players in managing security by design and default, driven in part by legal requirements relating to data protection by design and default. Moreover, as new product development lead times are relatively short reflecting the fast-moving nature of the industry, some stakeholders argued that security vulnerabilities that were more prevalent five years ago are much less of an issue today. This illustrates the difficulty in assessing the degree of risk at the product level, as the situation changes over time, as the industry's capabilities and maturity level to deal with existing known, and new security vulnerabilities evolve.

A further finding was that the way in which a particular internet-connected RE device is connected, either directly or indirectly to the internet, has a difference in terms of the associated level of risk. Directly- connected RE products are at greater risk than those indirectly connected. However, this is not to suggest that there is no risk associated with indirectly-connected devices. This complicates the question of determining which products should fall within the scope of the delegated acts, were these to be activated. A couple of product-specific examples regarding the complexities in regulating due to the fact that some products may be wired, and others wireless (both directly and indirectly connected) are provided below:

- **Smart alarms –** such alarms come in a variety of forms, including non-internet connected wired (outside the RED's scope), directly and indirectly connected.
- **Baby monitors and security cameras –** likewise, there are three types of products, Wi-Fi-enabled, where hacks have occurred and most of the vulnerabilities have been identified, IP-enabled only indirectly connected and low-medium frequency devices that are not internet-connected but where there are still some localised security risks.
- **Complex RE products arguably have higher risks associated with them than simple products.** The reasons for this are multi-faceted. For example:
  1. **Complex products, such as mobile phones and laptops are likely to have a more complex supply chain than simple products,** meaning that there may be more risks associated with the RE device. Such devices collect a variety of personal data on the device, and will typically have a wide number of different third-party pieces of software and app's. This means that there is complex responsibility across the supply chain and value chain for ensuring compliance with relevant EU legislation e.g. GDPR and e-PD. The value chain consists of the final manufacturer, chip component and other component / part manufacturers, as well as third-party pieces of software and app's that may be pre-loaded with the product but often downloaded by the user themselves post-market placement. As EU legislation currently stands, the RED is applicable pre-product placement, whilst the GDPR is applicable both pre-product placement (i.e. Art. 25 GDPR security by design and default under the responsibility of data controllers and processors) and post-product placement.
  2. **Ensuring GDPR compliance is often complicated in complex products both from the perspective of the final manufacturer and market surveillance and enforcement.** As there are complex value chains, there are typically a number of data processors under the responsibility of a data controller. This makes tracing responsibility for compliance – and to establish the source of any data breaches – arguably more difficult than for simple products.
  3. **More extensive personal data and identifiers are commonly collected compared with simple products.** Taking an example, considerably more personal data is collected via a laptop or mobile phone compared with say a robotic lawnmower only collecting data on product performance. Were there to be a data breach, therefore, the consequences in terms of data loss, risk of data theft and fraud, etc. are therefore commensurately higher. However, this does depend how complex products are defined.
- **The extent to which security vulnerabilities can be characterised according to whether a given product is complex or simple is somewhat nuanced**. Although there are differentiated risks, device penetration risks stem from being internet-connected. Moreover, the level of risk depends whether the device is assessed from the point of view of it being a standalone device in its own right, or as the weakest link in a home or enterprise network in which an unsecured device could provide a gateway into devices containing sensitive data.
- **There are however risks associated with downplaying the degree of risk of simple products.** Hackers may target individual simple connected RE devices as a gateway to accessing sensitive data, such as an attack on a fish tank's **smart thermostat** in a Las Vegas casino[115]. This helped hackers to gain access to the casino's network in 2018. This was one of several data breaches at the casino which allowed hackers to obtain the cardholder names, card numbers, and CVV

[115] This claim was made in a report released by cybersecurity firm Darktrace. See for example - https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4 and https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

numbers of hotel guests. Hackers are increasingly targeting IoT devices to find their way into corporate networks via the weakest link.

4.2.2.1 Market dynamics and the implications for security vulnerabilities

It is worth considering the role of competitive market dynamics in influencing how manufacturers deal with security vulnerabilities when under time and cost pressures, and whether there is a risk that without regulation, they may not always test their products thoroughly enough, or in accordance with their legal obligations relating to data protection by design and default. For example,

- Manufacturers of internet-connected radio equipment, especially of consumer IoT devices, where product markets are very fast-paced, operate in a market where there is growing competition with attendant pressures to decrease the time to market. This may risk some manufacturers taking security shortcuts to ensure that their product is launched on the European market quickly, absent any existing regulatory requirements.
- The price of many internet-connected RE continues to fall, putting cost pressure on producers, as consumers' expectations are that costs come down over time (e.g. of security cameras, mobile phones, laptops and other smart devices). This may have implications as to the level of investment in security that some manufacturers, especially those at the cheaper end of the market, are able to make.
- The above-mentioned factors could result in security vulnerabilities not being properly addressed through the integration of data protection by design and default (and the non-adoption of good practices in security by design and default principles). However, the research, especially the interview programme, suggests that this affects less well-known brands, and lower priced products in particular.
- This is not to suggest that there is a problem among all manufacturers, as many take their regulatory compliance obligations very seriously and are concerned about implementing broader security by design and default principles for other reasons, such as reputation management. It is rather a question of flagging up that not all manufacturers take product security seriously enough.
- The research also explored the extent to which consumer and enterprise-level internet-connected RE products and devices pose a greater or lesser risk. Although security vulnerabilities were more commonly identified at the product level among consumer- IoT products and devices, which tend to be cheaper, and therefore, more commonly lack authentication and encryption capabilities, some enterprise grade products are also at risk, as they may be better protected, but there are potentially benefits for hackers in gaining access to unauthorised personal data in a corporate environment, therefore risks remain prevalent.

4.2.3 Technical solutions

The research has identified a series of different types of technical solutions to improve the security of connected RE products falling under the RED’s scope. These range from the use of international technical standards, industry standards and manufacturers testing to their own internal security requirements and protocols, as well as the integration of security (and data protection) by design and default principles into the product design and engineering processes. Furthermore, the product case studies have identified a series of technical solutions to address specific security vulnerabilities, as well as common vulnerabilities across connected RE products.

Evidently, both the vulnerabilities themselves, as well as the technical solutions, are varied, multi-faceted and constantly evolving. In this report, it is therefore only possible to provide selected examples, drawing on the findings from the targeted consultations regarding which types of technical solutions manufacturers have deployed, and the feedback obtained through the interview programme, with particular reference to the product case studies.

4.2.3.1 Feedback on technical solutions from the targeted consultations

Feedback was obtained through the **targeted consultations** as to which types of technical solutions are being utilised. Manufacturers, economic operators and their organisations/associations were asked how they (or their members or affiliates) currently ensure that "data protection by design & default" requested in Art. 25 of the GDPR is taken into account regarding the products that they place on the EU market. Of those offering a response, slightly more than half used international standards, whilst the rest used internal procedures. Reference should be made here to the standalone annex setting out the findings from the targeted consultations.

When asked to specify, respondents referred to the following standards to ensure that their products, business processes and procedures were compliant with any legal obligations (e.g. Art. 25 data protection by design and default), as well as aligning with good practices in respect of security by design and default principles:

- ISO/IEC 27000 series, which is not linked to a sector but is relevant for connected devices, e.g. ISO-IEC 27001.
- IEC 62443-X series, e.g. IEC 62443-4-1, which specifies the process requirements for the secure development of products used in industrial automation and control systems.
- ETSI TS 103 645, addressing cybersecurity for the consumer Internet of Things.

When asked to comment on their use of standards, the respondents stated the following:

- One industry organisation highlighted that cable operators procure cable modems and cable modem termination systems that are built in conformity with the CableLabs' DOCSIS specifications. These are approved by the International Telecommunication Union (ITU). They include a multitude of security controls to help ensure the confidentiality, integrity, and availability of cable broadband services.
- One industry association reported that the lighting industry is relatively new in this field and that requirements are only starting to be applicable.
- Another industry association recommended that standards should not differentiate between different categories of product (e.g. children’s toys) but by functionality.
- One industry organisation reported that approaches to ensuring security are evolving rapidly, as evidenced, for example, by the rapid adoption of two-factor authentication in connected devices in recent years.

Were the two delegated acts to be activated, several respondents agreed that the development of harmonised standards listed in the OJEU providing presumption of conformity would be key for manufacturers to ensure that their products were compliant with baseline security requirements.

4.2.3.2 Feedback on technical solutions from the product case studies

The product case studies identified a diverse range of potential technical solutions to address identified security vulnerabilities in connected RE products. It is important to note that, in the same way that some vulnerabilities are common across all categories of connected radio equipment (by dint of being internet-connected), there are equally technical solutions relevant across all types of RE products. Notwithstanding, there are also examples of technical solutions that address particular vulnerabilities in specific classes of products.

Perhaps the best example of technical solutions that could potentially resolve a lot of security-related problems with connected RE that would help to strengthen and safeguard data protection and privacy and to prevent fraud are the **integration of authentication and encryption technologies** from the outset of the design process. Before considering this, it is worth providing a short overview of the types of security protocols and technologies that are already available.

Box 4.5: Typology of authentication and encryption

Authentication

The process or action of verifying the identity of a user or process.

General authentication techniques

- Passwords, two-factor authentication [2FA], tokens, biometrics, transaction authentication, computer recognition, CAPTCHAs, and single sign-on [SSO])

Specific authentication protocols

- Examples are Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are cryptographic protocols that authenticate data transfer between servers, systems, applications and users.
- Trusted User Interfaces (TUIs) for securing critical mobile apps. It supports mobile authentication & biometrics. A TUI can be a specific mode in which a mobile device is controlled by the trusted execution environment (TEE) a secure area of a main processor in a smartphone (or any mobile device) which ensures that sensitive data is stored, processed and protected in a trusted environment.

Encryption

- Encryption technologies can be applied at various levels in a piece of connected RE, e.g. in chips, in hardware (especially data storage), in software and in communications tools relating to the transmission of data from the device (e.g. secure messaging and email systems).
- Encryption protects data by scrambling it using an encryption key with a randomly generated passcode. In theory, without the key, third parties would be unable to view the data. However, hackers can attempt to steal access by impersonating an authorized user. Encryption authentication.

Examples are:

- Use of chips with encryption capabilities.
- Encryption protects data by scrambling it with a randomly generated passcode, called an encryption key.
- Hardware security module (HSM) containing one or more secure crypto processor chips (note - often used with enterprise-grade servers)
- Use of encryption algorithms
- Cryptography
- Rating of password strength
- Encrypted storage
- Encryption of files/folders
- Encryption of text
- Secure deletion capabilities
- Trusted Platform Modules (TPM) - implementation of a secure crypto processor that brings the notion of trusted computing to ordinary PCs by enabling a secure environment.

Network security protocols

- Ensuring that RE devices use network security protocols, such as the use of Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL).

4.2.3.3 Technical solutions identified by the European Standards Organisations (ESOs)

During the course of this IA study, the ESOs (ETSI, CEN and CENELEC) have been asked by the European Commission to carry out a preliminary review and screening to identify what sorts of technical standards and other sorts of technical solutions might already be available. These could then be used if the two DAs were to be activated. This has led to some 150 different technical standards that already exist being identified, although for these to be operable, they would need to be translated into European harmonised technical standards.

ETSI, CEN[116] and CENELEC have also been undertaking work to identify suitable possible technical solutions and existing international standards that could be utilised as the basis for work to begin on the organisation of harmonised technical standards. In the following table, selected examples of standards are provided:

Table 4.3: List of technical solutions prepared by experts from CEN/CLC/JTC 13/WG 6.

Status	Reference	Title	Rationale and considerations
Working draft	ETSI EN 303 645	Cyber Security for Consumer Internet of Things. Securing Consumer IoT	New standard for consumer IoT. Integrates 13 main principles relating to security by design and default.
Published	IEC 62443-3-3:2013	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels	Widely accepted standard for evaluation of security of ICS/SCADA and building automation system security, which has broad horizontal applicability.
Published	IEC 62443-4-1:2018	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements	Widely accepted standard for evaluation of security of ICS/SCADA and building automation components security, which has broad horizontal applicability.
Published	IEC 62443-4-2:2019	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components	Widely accepted standard for evaluation of product development lifecycle of organizations building ICS/SCADA and Building automation device/systems, which has broad horizontal applicability.
Published	ISO/IEC 20924:2018	Internet of things (IoT) – Vocabulary	
Published	ISO/IEC 30141:2018	Internet of Things (IoT) – Reference architecture	
Working draft	ISO/IEC 27030	Guidelines for security and privacy in Internet of Things (IoT)	The standard will provide guidance on the principles, [information] risk and controls for IoT security and privacy.
Published	ISO/IEC NP 30147	Information technology — Internet of things — Methodology for assessing the trustworthiness of IoT system/service	

[116] The longlist of possible standards was prepared by experts from CEN/CLC/JTC 13/WG 6.

Status	Reference	Title	Rationale and considerations
Published	ISO/IEC 29147:2018	Information technology – Security techniques – Vulnerability disclosure	[Process] Part of manufacturers due diligence.
Published	ISO/IEC 30111:2013	Information technology – Security techniques – Vulnerability handling processes	[Process]
Published	ISO/IEC 27032:2018	Information technology — Security techniques — Guidelines for cybersecurity	
Published	ISO/IEC TR 27013:2018	Information technology — Security techniques — Cybersecurity and ISO and IEC Standards	This TR provides an overview of ISO/IEC standards that can be applied for Identify, Protect, Detect, Respond and Recover.
GPC_SPE_034	Card Specification V2.3.1	Standard to deploy and manage application in embedded Secure Component (like banking card, SIM, eSIM …).	
Published	GPC_SPE_007	Confidential Card Content Management – Amdt A V1.2	Additional feature for of the GPC_SPE_034 for management by several entity with delegation.
Published	GPC_SPE_011	Remote Application Management over HTTP – Amdt B V1.1.3	Additional feature of the GPC_SE_034 for management over HTTP.
Published	GPC_SPE_025	Contactless Services – Amdt C V1.3	Additional feature of the GPC_SE_034 for the contactless transaction (in near field communication).
Published	GPC_SPE_014	Secure Channel Protocol '03' – Amdt D V1.1.2	Additional feature for GPC_SE_034 allowing secure channel protocol with AES cryptography.
Published	GPC_SPE_093	Secure Channel Protocol '11' – Amdt F V1.2.1	Additional feature for the GPC_SE_034 for secure channel based on Asymmetric Cryptography Algorithm. Enabling also mechanism for a deployment from a single entity (like a digital store).
Published	GPC_SPE_106	Opacity Secure Channel – Amdt G V1.0	Additional feature for the GPC_SE_034 enabling privacy for end-user.
Published	GPC_SPE_120	Executable Load File Upgrade – Amdt H V1.1	Additional feature of the GPC_SPE_120 allowing to upgrade application when keeping the deployed specific data.
Published	GP_REQ_025	Root of Trust Definition and Requirements V1.1	Definitions and Requirements for developing Root of Trust software/firmware.
Published	ELF Upgrade – Amdt H V1.1 Compliance Test Suite V1.0.0.1	Compliance for Amdt H	
Published	SCP11 – Amdt F v1.2 Compliance Test Suite v1.0.0.1	Compliance for Amdt F	

Status	Reference	Title	Rationale and considerations
Published	SE Configuration V2.0 Compliance Test Suite V1.7.0.1	Compliance for a Secure Element configuration covering a set of specifications for an homogenous configuration.	
Published	Common Implementation Configuration V2.0 Test Suite V2.1.0.1	Compliance for a Secure Element & UICC configuration covering a set of specifications for an homogenous configuration.	
Published	Financial Configuration V1.0 Compliance Test Suite V1.1.0.1	Compliance for a banking product configuration covering a set of specifications for an homogenous configuration.	
Published	GPD_SPE_008	Device API Access Control V1.0	Ensure application limitation of device API accessing to the applications running in secure environment (and protection from denial of service).
Published	GPD_SPE_075	Open Mobile API Specification v3.3	Ensure application limitation to access to the applications running in secure environment (and protection from denial of service).
Published	GPP_SPE_004	Open Mobile API Test Specification for Transport API V3.3	Ensuring compliance for the GPD_SPE_075.
Published	GPD_SPE_009	TEE System Architecture V1.2	Defining architecture for a Trusted Execution Environment.
Published	GPD_GU_125	OTrP Profile Initial Configuration V1.0	Open Trust Protocol allowing a management and deployment of application for a Trusted Execution Environment.
Published	GPD_SPE_120	TEE Management Framework including ASN.1 Profile 1.0.1	Framework allowing management of Trusted Application.
Published	GPD_SPE_123	TEE Management Framework: Open Trust Protocol (OTrP) Profile 1.0	Framework allowing management of Trusted Application (but for OTrP).

The table shows that there are a number of different types of authentication technologies such as Trusted User Interface (UI) API v1[117], the standard for secure digital services and devices. A Trusted UI is a specific mode in which the user interface of a device is controlled by the Trusted Execution Environment (TEE), an isolated area in the main processor of a smartphone (or any connected device). This ensures that sensitive data is stored, processed and protected in a trusted environment. The Trusted UI ensures that malware running in the device cannot tamper with displayed messages, capture secret information displayed to the user and intercept PINs or passwords entered by the user, as in a 'PIN on Glass' scenario. It also prevents malware from running transactions without explicit user consent."

Biometric authentication can secure the hardware of a smart device using TEE. APIs enable trusted applications to leverage say a phone device's biometric sensors. They can remain fully isolated from the device's Operating System (OS), and trusted user interactions can be fully configured to meet the

[117] Trusted User Interface API v1 https://globalplatform.org/specs-library/trusted-user-interface-api-v1/

specific needs of each digital service. Regarding use cases, such technologies could be deployed for example to ensure a secure connection between a connected car and a device such as a mobile phone or other smart device[118].

A series of IT security techniques have also been identified such as **vulnerability disclosures**, vulnerability handling processes and guidelines to address security vulnerabilities. Indeed, DG CONNECT has stressed the importance of monitoring vulnerability disclosures in the CSA in relation to the development of product-specific certification schemes as it ought to inform standards developers about what are the main threats and vulnerabilities. ENISA has assumed this role.

Some of the technical solutions identified focus on consumer IoT and industrial IoT. Consumer IoT is one of the main areas that regulators and standardisation bodies globally have been focusing on. Examples are the development of ETSI TS EN 303645 (Cyber Security for Consumer IoT), released in February 2019. This contains thirteen principles relating to security by design and default, only some of which are relevant to the RED's scope i.e. at the point of placing products on the European market. The inclusion of three of these good practice principles embedded in ETSI TS EN 303645 is also being considered by the DCMS in the UK as part of a possible regulatory approach (see Section 3.3.6 - National developments in the EU and third countries).

The level of **security in consumer IoT products and devices** tends to be less well developed than for enterprise-grade products. This is because enterprise clients demand better security and performance functionality and will pay more for the product (e.g. laptops, routers). This allows manufacturers chance to integrate improved security features, such as the encryption of hardware (including chipsets and microprocessors), and the use of encryption in software and network communications. In addition, more expensive enterprise products may provide a secure vault within storage space (e.g. laptops).

In the US, NIST has also been working on the development of baseline requirements for IoT devices targeted at IoT device manufacturers. Again, the focus has been on prioritising the risks associated with security vulnerabilities in consumer IoT devices. The assessment of existing technical standards also identified examples of technical solutions that could be used to strengthen security in respect of other types of internet-connected RE and wearable RE. Examples are international standards, such as IEC 62443-4-1:2018 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.

A case study example on the world's first standard for consumer IoT security is provided below.

Box 4.6: Case study 3- Review of existing Technical Solutions to Strengthen Consumer IoT security (ETSI TS 103 645)

Rationale for the development of a standard covering cybersecurity for consumer IoT

Ensuring cybersecurity of the IoT is becoming a growing concern as an increasing number of consumer devices in the home are connected to the internet. According to HIS Markit, the number of IoT devices globally will increase from 27 billion in 2017 to 125 billion by 2030.[119] Whereas 10 years ago, most electrical and electronic products, and many household appliances, could be classified as "simple products", they are now increasingly smart, connected to the internet (either directly or indirectly) and networked. The transition to more complex, smart products means these need to be designed to withstand cyberthreats.

Market surveillance authorities reported during the interview programme that many IoT product lack the integration of even basic cybersecurity considerations, with practices such as the use of common default passwords remaining common. Lack of adequate attention to security by design and default

[118] Focus on use case of a connected car - https://globalplatform.org/use-case/connected-car/

[119] Howell, J. (2017). Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says. https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says

principles during the product development process was identified as being a major problem, by stakeholders such as MSAs, European and national consumer associations and by cybersecurity professionals interviewed.

Description of technical solution(s)

In light of the emergence of growing cybersecurity risks for consumers associated with the placing on the market of consumer IoT devices that do not meet acceptable levels of basic cybersecurity, a need was identified by ETSI for the development of a common framework setting out minimum baseline security requirements for all consumer IoT devices. Accordingly, in February 2019, the ETSI Technical Committee on Cyber Security (TC CYBER) released Standard ETSI 103 645 to improve consumers' privacy, digital security and safety. ETSI 103 645 is aimed at strengthening cybersecurity in consumer IoT not only by establishing a security baseline for internet-connected consumer products, but also by providing the basis for the future development of IoT certification schemes.

The aim of ETSI 103 645 was to provide a general framework on consumer IoT security which could lay the basis for the subsequent development of technical standards, specific to different types of consumer IoT products and devices. The TS built on the "Code of Practice for Security in Consumer IoT Products and Associated Services" published by the Department for Digital, Culture, Media and Sport (DCMS) in the UK.

Scope of ETSI 103 645

Economic operators responsible for developing, producing and selling connected consumer IoT products are the main target audience for the standard. The types of products where such a standard might be relevant in setting out the general principles for cybersecurity requirements (with more detailed product-specific minimum baseline requirements then being developed are *inter alia*: children's toys, smart cameras, connected household appliances, etc). The standard contains approximately a dozen high-level outcome-focused requirements, which draw on accepted good practices in IoT security.

Relevance to the RED: The 12 principles set out in the ETSI standard are highly relevant to tackling different problems and vulnerabilities from a cybersecurity perspective. However, these principles reflect a lifecycle approach to maintaining high levels of cybersecurity from the product design stage and the integration of security by design and default principles to post-placement on the market.

Examples of these principles are:

- **Banning the use of default passwords;**
- Having the means to manage identified cybersecurity vulnerabilities;
- Keeping software updated and notifying consumers of these updates;
- **Ensuring secure communication of sensitive data through encryption;**
- Ensuring the secure storage and management of keys;
- Using approaches such as secure boot to ensure the integrity of software;
- Making sure devices are resilient to outages.

It is therefore important to highlight that only some of these principles are relevant to, and fall within the RED's scope. Those especially relevant to the RED are highlighted above.

Potential effectiveness and utility of the technical solution(s). A key issue is how useful ETSI TS 103 645 could be in providing an example of a workable technical solution to enhance cybersecurity in general, and data protection and privacy and protection from fraud in particular. Were the two delegated acts to be activated or alternatively, if an industry-led approach were to be adopted, this technical standard (TS) could be useful.

Accordingly, feedback was gathered through the stakeholder consultations as to how useful and potentially effective the TS is likely to be in future. Stakeholders agreed that the development of the

ETSI standard is an important starting point towards the development of minimum baseline (cyber)security standards for consumer IoT devices, as it follows ‘security by design and default’ principles. Member States also find it helpful because it will be possible to build on the standard and to add new security elements.

Possible limitations:

- A stakeholder from a national notified body pointed out that ETSI TS 103 645 seeks to ensure that consumer IoT products integrate basic cybersecurity requirements into device and product functionality, but it does not set out any detailed technical specifications. More detailed technical standards and solutions to be implemented would subsequently need to be developed on a product/ device-specific basis. Such standards would need to be published openly and then evaluated/ tested and would also need to reflect ‘state of the art’.
- Stakeholders pointed out that whilst the ETSI TS embodies a number of good practice principles, but only some fall within the RED’s scope. The **ETSI standard sets out a framework for the full product lifecycle and concerns the entire IoT ecosystem**, whereas the RED only covers the period leading to the product’s placing on the market.
- Therefore, whilst useful in providing guidance to manufacturers as to how to implement security by design and default principles, there would only be scope to include some principles as technical solutions to help implement a possible future Delegated Act. Examples are: outlawing the use of default passwords, and ensuring the secure communication of sensitive data through encryption built into IoT devices. Such measures would strengthen the cybersecurity of consumer IoT devices at the design phase and before they are placed on the market. A major pan-European and global manufacturer of electrical products interviewed commented that *“Whilst the ETSI TS is a good starting point, a number of the requirements could not be addressed within the scope of the RED, because they concern post-product placement and process requirements”.*
- Under a risk-based approach, the costs of going beyond minimum baseline **security requirements may be prohibitive.** If a risk-based approach were to be adopted, which went beyond minimum baseline security requirements, there could be a question mark as to whether higher-risk products could continue to use the Self-Declaration of Conformity (SDoC) approach presently allowed for all product categories under the RED.
- If mandatory third-party testing were required for products identified as posing a higher level of risk, and therefore requiring higher-level cybersecurity requirements, then the costs of such high-level security requirements could be such that they may limit market access for lower volume products.

Lessons learned:

Since the TS was only published in February 2019, it is perhaps premature to learn lessons. However, various observations were made:

1. Interview feedback suggested a need for **the piloting of ETSI TS 103 645 at the product group level** to ascertain whether the approach is likely to be effective. Without further piloting, the feasibility of translating the umbrella ETSI TS into setting minimum baseline requirements for particular product groups cannot be known. It could therefore be difficult to make the TS mandatory immediately.
2. Conversely, some stakeholders suggested that **without regulatory requirements making the implementation of minimum baseline cybersecurity standards mandatory, industry may generally be reluctant to take action**, or to make the investments to strengthen cybersecurity. An exception in this regard is that some large industry players have made enhanced cybersecurity product features part of their sales and marketing strategies.
3. The importance of **securing acceptance from industry of the ETSI TS to ensure wide take-up** was stressed. Rather than issuing standardisation mandates to ETSI for particular product groups (stemming from the possible activation of one or more delegated acts under the RED), it was suggested that existing industry initiatives to develop technical solutions should be

checked since these could provide an alternative mechanism to issuing a new standardisation mandate to ETSI, based on the ETSI umbrella standard. An example provided was that in the fields of Wi-Fi and WLan[120] and Mobile Phone cybersecurity, industry already drives standardisation processes, and it was seen as being important not to reinvent the wheel.

Other guidelines for industry and Technical Solutions to enhance cybersecurity:

The ETSI TS is comprised of common-sense principles relating to security by design and default and to ensuring cybersecurity throughout the product lifecycle.

It is worth pointing out that there are wider guidelines available pertaining to consumer IoT security, such as:

- EU Cybersecurity Act - the creation of an EU ICT security certification framework for products and services. Certification schemes will use standards and technical specifications to both express as well as assess conformity to specified cybersecurity requirements.
- Technical Committee 30 CEN/CENELEC 6 has been considering how to approach standardisation from a cybersecurity perspective. A Feasibility study was undertaken on the introduction of basic cybersecurity requirements.
- The IoT Security Foundation has published a White Paper mapping IoT security functionality[121].
- ENISA – baseline security recommendations for IoT in the context of critical information infrastructures
- ENISA – product-level certification schemes relating to cybersecurity being developed under the (voluntary) Cybersecurity Act
- Department for Digital, Culture, Media and Sport, UK – Secure by Design: Improving the cyber security of consumer Internet of Things report
- DCMS – Industry Code of Conduct on Consumer IoT Security, November 2018
- IoT Security Foundation – IoT Security Compliance Framework
- GSMA – IoT Security Guidelines and Assessment

Source: desk research, interviews with industry associations and manufacturers.

Standards and certification will also play an important role under the Cybersecurity Act (CSA), although it will take time for the ESOs to develop new standards as ENISA is envisaging gradually rolling out standards on a product by product basis. Although voluntary, such schemes could help to harmonise cybersecurity certification throughout the EU and thereby eradicate single market barriers. The certificates are also meant to allow users to develop a better understanding of the security features of products or services they want to purchase, therefore contributing to greater market transparency. Each certification scheme will specify which categories of ICT products, services and processes covered, and develop tailored cybersecurity requirements.

The European Commission's initiation of a **framework for cybersecurity certification** [122] could provide useful technical standards and supporting certification that could also be of use were the two DAs to be activated. The type of evaluation of a particular product, service or process will be outlined (e.g. whether conducted through self-assessment or by a third-party testing and inspection body) and the intended level of assurance. This could provide a model for future harmonised technical standards to be developed if the delegated acts were to be activated.

[120] Many improvements in standards have been made by industry in respect of privacy for product groups such as WiFi and the W-LAN protocol (IEEE 802.11). If these protocols become more standardised across the industry in a particular product type, then this could serve to improve privacy.

[121] Mapping the IoT Security Foundation's Compliance Framework to the DCMS proposed Code of Practice for Security in Consumer IoT. IoTSF Working Group Document, 2018. Available from https://www.iotsecurityfoundation.org/wp-content/uploads/2018/03/RELEASE-DCMS_Principles_Application_Note_07_03_2018.pdf

[122] European Commission, (2017), The EU cybersecurity certification framework. Published September. Available at: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

The delegated acts within scope do not cover cybersecurity in its broader sense but address security vulnerabilities relating to a lack of safeguards for data protection and privacy and protection from fraud. Nevertheless, harmonised technical standards relevant to Art. 3(3)(e) and 3(3)(f) will still need to consider aspects of cybersecurity, as without sufficient protection to prevent the unauthorised penetration of internet-connected RE and wearable RE to avoid data breaches, it will not be possible to ensure such RE is secure.

Through the mapping and documentation of their business processes, which is already required under the GDPR (e.g. Art. 25 and Art. 24), manufacturers could make clearer what security measures and functionality had been integrated into RE products, and across which aspects of the systems architecture (segregation between different processors e.g. radio processors, application processors, memory processors and other types of processor and in the design of control systems to manage these processors). This would in turn make it easier for users to take steps to protect themselves and avoid device and network-level breaches that could compromise the personal data on a device. Therefore, whilst standards play a valuable role in the CSA, certification goes beyond this and encourages better communication of security-related issues to the end user. This could be a useful overall approach when considering how to develop appropriate harmonised technical standards, were the two delegated acts to be activated through the RED.

4.2.3.4 Security standards to prevent fraud

Research was undertaken to identify whether there were any specific security standards to prevent fraud. As safeguards to ensure protection from fraud is a new area in the standardisation field compared with other security areas, there is a lack of a definition of fraud in the RED, it was important to check which types of standards are available.

The main findings were, in summary that:

- There are some examples of security standards to ensure protection from fraud, but these mainly focus on ensuring strong security in new payment systems, such as contactless. Indeed, security standards in payments have been around for many years, but have been updated to reflect the emergence of new technologies, such as contactless;
- There is also software available to protect against identify theft, but this is mainly for use in an internet browser context, rather than built in to internet-connected RE and wearable RE directly;
- The prevention of fraud at the device level is more dependent on taking steps to build in security functionality to the hardware and software on the device, but cybersecurity standards, along with encryption and authentication will help to prevent fraud, along with make the RE less easy to penetrate when the device or product is directly (or indirectly) connected to the internet.
- When developing minimum baseline security requirements under the RED to protect against fraud, security standards developed to ensure the security of payments are an example of how industry-driven standards could inform the development of European harmonised standards.

More detailed examples to support these findings are now provided.

Firstly, examples of technical security standards are provided. The **PCI PIN Transaction Security Point of Interaction (PCI PTS POI) Standard** has enabled contactless payments for many years and provides security requirements for mobile and other devices that are purpose-built for payments.

A new security standard called Contactless Payments on COTS (commercial off-the shelf devices), or the PCI CPoC initiative was recently developed by the PCI Security Standards Council. [123] CPoC expands support for contactless payments with a new data security standard specifically for contactless acceptance on merchant COTS devices. The standard enables retail merchants to accept contactless

[123] https://blog.pcisecuritystandards.org/just-published-pci-contactless-payments-on-cots

payments using a smartphone or other commercial off-the-shelf (COTS) mobile device with near-field communication (NFC) technologies. Security and Test Requirements for contactless payments on COTS was published in December 2019. [124]

Security standards developed by industry to ensure security of payments (and thereby prevent fraud) provide examples of appropriate technical solutions already accepted by industry in Europe and globally that could be useful in providing minimum baseline security requirements under the RED.

The CPoC initiative is part of the Council's mission to enhance global payment data security by developing standards that *"support secure payment acceptance in new and emerging payment channels. Ultimately, the PCI CPoC Standard and Program will lead to more options for merchants to accept contactless payments in a secure manner".* [125] In other words, it is recognised in the FinTech industry that new payments technologies would secure broader acceptance if there are security standards in place. The industry is therefore already investing in such standards. Such technical solutions could then provide a useful example of a security standard that could be incorporated within a future harmonised technical standard at EU level if Art. 3(3)(f) were to be activated. This would then ensure that payments made using certain categories of internet-connected RE are secure.

A further example of a security standard to prevent fraud is a standard setting minimum data security requirements to be met by any organisation that transmits, processes or stores payment card data. The standard involves combining EMV chip card technology and the PCI standard [126] to provide protection based on authentication and data control.

However, beyond secure payments, there are not many technical standards specifically focused on other types of prevention against fraud. For instance, it is difficult to legislate for protection against identity fraud, rather, it may be appropriate to produce and disseminate good practice guidance as to how users of internet-connected RE and wearable RE can protect themselves. There have been previous initiatives to prevent users against the theft and misuse of personal and financial information. For example, in 2008, the Identity Theft Prevention and Identity Management Standards Panel (IDSP) created a comprehensive resource of standards, guidelines, and best practices related to identity theft and fraud prevention. This was developed through a partnership of more than 70 organisations from the public and private sectors. The report by the IDSP considers the life cycle of identity management from the issuance of identity documents by government and commercial entities, to the acceptance and exchange of identity data, and the ongoing maintenance and management of identity information. [127]

There are products available to protect consumers in their online activities against identify theft and related fraud. However, these relate less to technical measures and more to monitoring to protect data mis-use. For example, a well-known anti-virus protection firm [128] provides Cyber Monitoring of digital black markets on the internet and Dark Web for personal data and information such as email addresses, credit card numbers, etc. Customers are then alerted if any suspicious activity is detected.

Preventing fraud effectively can therefore either be done by regular monitoring to detect any fraudulent activity, or better to prevent device penetration from occurring in the first place. The latter however relies on authentication and encryption technologies and on security measures to prevent unauthorised third-party access, which could also prevent data loss and privacy breaches, as there is a lack of specific standards on fraud.

[124] Security and Test Requirements for contactless payments on COTS, December 2019.
https://www.pcisecuritystandards.org/documents/Contactless_Payments_on_COTS-Security_and_Test_Requirements-v1.0.pdf?agreement=true&time=1584710658623

[125] https://blog.pcisecuritystandards.org/just-published-pci-contactless-payments-on-cots

[126] https://www.welivesecurity.com/2016/12/12/combining-technology-standards-combat-fraud/

[127] https://www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08

[128] https://www.mcafee.com/en-us/identity-theft/protection.html

For any future harmonised technical standards to be effective, there will need to be a high level of adoption by industry. This could be more easily ensured under a regulatory approach, as although standards are voluntary, they are the preferred means of complying with the essential requirements for many manufacturers.

4.2.4 Synthesis assessment - issues relating to the collection and processing of personal data

Section 4.2.2 considered technical security vulnerabilities due to device penetration, such as malware, other forms of hacking, etc. It is also important that non-technological issues relating to data protection and privacy, and protection from fraud are also analysed. Although many vulnerabilities can arise from business processes and personnel, such as insider threats, the most pertinent question in relation to this analysis concerns what types of personal data are legitimately being collected by manufacturers, software/ app developers and other third parties involved in big data value chains and if data collection is being carried out with users' consent in an IoT world, as legally required under the GDPR. Following this, it is also necessary to consider whether the GDPR is sufficient to prevent data misuse.

The analysis presented in this sub-section draws on desk research, interviews and the findings from the product-based case studies and considers whether data being collected by manufacturers and third parties, such as software developers, are legitimate. Any instances where users' data might be used in an unethical way are also considered. In other words, whilst a robust legal framework is in place through the GDPR, how far there remain problems that could necessitate activating the delegated acts is considered.

The following questions are explored in this sub-section:

- What type of personal (and non-personal data) is being collected by manufacturers and other firms involved in the data value chain legitimately from typical internet-connected RE products?
- Are there any examples of data misuse across different internet-connected RE products? If yes, do these precede the GDPR's coming into effect and how far have business practices changed?
- Is personal data being collected in a way that is legally-compliant with the GDPR? For instance, how transparent and ethical is data collection post-GDPR?
- Are users aware about the particular specific uses they have given their consent to, and are there particular challenges in this regard due to the particularities of consumer IoT devices as opposed to the more traditional internet?
- Is the absence of a clear user-interface to provide consent for some types of internet-connected RE products problematic?

What type of personal (and non-personal data) is being collected by manufacturers and other firms involved in the data value chain legitimately from typical internet-connected RE products?

The product-based case studies (presented in full in Annex 8) contain information regarding what type of data (personal, non-personal) about the product's functionality and performance is being collected by each of the six products selected for case studies (seven in that one case study covers two related product groups (baby monitors and security cameras). An overview of the findings is provided below:

Table 4.4: Types of personal and non-personal data

Product group	Type of personal and non-personal data being collected
Laptops	• Laptops, along with products such as mobile phones, are a complex product with multiple and different types of processors (e.g. radio processors, application processors, and memory processors. • Extensive personal and non-personal data are collected, stored or processed by laptops,

Product group	Type of personal and non-personal data being collected
	including by the operating system (OS) and many applications installed on the laptop as well as through websites accessed via the internet. • Furthermore, data collected by individual connected RE products may be transferred via the laptop. These data could include any data collected by RE products, for example activity data from wearables. • In addition, users store significant amounts of personal and non-personal, commercial and private data on their laptops (e.g. this could include a company's financial data or an individual's private photos or videos etc.). • As such, device breaches could lead to significant data loss either through a wireless connection (under the RED) or through other form of data theft (outside the RED's scope but a real risk, i.e. via a memory stick). • However, as data is collected on different processors, there is scope to design systems architecture in a way that maintains data security by building in the segregation of data collected via different processors.
Routers (wireless)	• Routers only collect limited personal data directly and there is limited data stored on the device itself, mainly technical performance data related to the device rather than personal data. • Non-personal information regarding the router's running status may be transmitted back to the producer, such as the number of devices connected to the router, types of connections, LAN/WAN status, Wi-Fi bands and channels, serial number, and technical data about the functioning and use of the router and its Wi-Fi network. Some limited personal data is also transmitted e.g. IP address, MAC address. • Various security vulnerabilities have been identified in routers . • The router may provide access to a home or office network which could include personal data being transmitted via individual RE products connected to the network via the router. There are therefore implications in terms of data protection and privacy, and non-protection from fraud if routers are not adequately secured. • Sometimes, relatively simple steps can be taken to secure routers, such as ensuring that the default password is changed, and that weak passwords are avoided. However, other security vulnerabilities and flaws are of a more technically complex nature.
(Connected) Security Cameras and Baby Monitors	• Security cameras (CCTV) and baby monitors capture images through video, still images and sometimes also audio. • Wi-Fi connected products pose risks of the products being breached. As the data is of a very sensitive and personal nature, for example, video footage of babies and children, if there is inadequate online security to secure access to the device, there are data protection / privacy issues. • There are some specific issues regarding the deployment of "facial recognition" technologies used by latest generation security cameras in public spaces. There are increasingly complex ethical issues which may in future require review as to whether regulation is fit for purpose to address these. • Facial recognition systems are used to identify individual by matching the face in the image captured live through a camera with images of faces stored in a database, through similarity in facial features. This is a controversial technology from a privacy perspective. • The issue of obtaining consent (as defined in the GDPR) remains an area of legal uncertainty as people in public places cannot provide consent to be monitored. Indeed,

Product group	Type of personal and non-personal data being collected
	according to a recent pronouncement by the Commissioner from DG CNCT, given the privacy implications, EO should hold back in deploying facial recognition technologies until GDPR compliance has been addressed. [129] Notwithstanding, she notes that there are exemptions to the rule with regards to public security issues, in which cases facial recognition technologies should be allowed to automatically identify persons legally. • How a public space is defined is also an issue. For example, if citizens install security cameras that takes images of visitors to their property, they should obtain consent to store the image.
Smart Toys	• The type of personal data collected by smart toys includes data linked to the initial account registration process, such as the name, gender, age, address etc. of the user (or their parent). In addition, some toys may have recording capabilities to record, capture and retain voice messages. • Localisation data i.e. data on the geolocation of the child using the smart toy may also be kept if the toy integrated with a RE device contains GPS/ location-tracking capabilities. Whilst such data is protected by the GDPR to ensure children's privacy, there remains the risk of malevolent attempts at third-party access if toys do not build in basic security requirements, such as user authentication.
Smart TVs	• Personal data collected includes the TV's IP address; the device ID and data on software updates (which provides information on whether the consumer has updated their device or not). Their security system covers three layers: applications, data and data transmission. • Consumers can voluntarily register their device online, after which the manufacturer stores some personal data about consumers. • If the manufacturer intends to collect and process personal data either themselves, then they would be subject to the GDPR and designated as the data controller. If they choose to reach agreements with third party service providers in the supply chain to provide services on a revenue-sharing basis, [130] then all third-party data processors would fall under the manufacturer's overall responsibility as data controller. • Manufacturer interviewed noted that they collect as little personal data as possible from consumers, however, third-party service providers from which the user may choose to install software, applications, smart devices connected to the TV) collect large amounts of information and data about users' viewing habits and preferences, and utilise this data to personalise content both to provide a customised user experience and for advertising purposes.
Smart Watches	• Smartwatches and wrist-worn fitness trackers contain extensive personal data, some of which is highly sensitive (e.g. children's geo-location, patients' medical information). • For example, smartphone health apps and consumer and medical wearable devices can measure almost every health metric, including heart rate, blood pressure, respiratory rate and blood glucose level. They can also detect and monitor diseases. • Personal data may in some cases be transmitted without using encryption. • Personal data collected also includes geo-locational data, which may if unauthorised

[129] https://www.euractiv.com/section/digital/news/vestager-facial-recognition-tech-breaches-eu-data-protection-rules/

[130] The manufacturer may allow a third party to install product software on the device prior to it being placed on the European market to allow data collection and processing by data processors and then share the commercial benefits.

Product group	Type of personal and non-personal data being collected
	access is gained pose a risk to the user, especially children. [131] - There have been examples of products that have been identified as being hackable as well as actual hacks. [132] - The research by Sophos notes that "higher-end products will typically have a much greater resistance to cyber threats than lower-end alternatives". - In 2015, Trend Micro issued a report which highlighted a major issue with the security of smartwatches: physical protection of sensitive data was lacking yet data was saved locally when the device was offline. Physical protection mechanisms need to complement the prevention of online device penetration. Otherwise, the devices remain insecure.

Are there any examples of data misuse? If yes, do these precede the GDPR's coming into effect and how far have business practices changed? Is personal data being collected in a way that is legally-compliant with the GDPR? For instance, how transparent and ethical is data collection post-GDPR?

Since May 2018, users of connected RE devices have been protected by the GDPR, including in respect of personal data misuse. In the era of big data-driven business models, manufacturers collect an array of data legitimately and process this as part of big data analytics. Data controllers and processors fall under the GDPR; however, there remain challenges, such as ensuring that consumers and other users are aware of what data is being collected, by whom and for what purpose, as well as ensuring that data is not misused once collected. The issue of user consent, a legitimate lawful basis for the processing of personal data under the GDPR (Art. 6), raises problems in an IoT context according to several pieces of literature consulted (see bibliography, Annex 1). For instance, a challenge that applies to many internet-connected RE devices is the absence of a simple user interface through which a user can provide consent. As such, it is less a question of whether there is legal protection (there is through the GDPR), but more a practical question of how manufacturers can make consent easy and meaningful (not just initial consent, but also as regards agreeing to, for example, changes in the processing).

As some of the product case studies make clear, value chains for some smart devices falling under the RED are complex, with a variety of economic operators involved in the production of the products, as well as the collection and processing of personal data once they are on the market. These stakeholders include manufacturers, third-party software and app developers, and service providers. This complexity brings manufacturers the added challenge of ensuring users' data is protected throughout the value chain. Furthermore, the systems and processes used by many data controllers to collect and analyse personal and other non-personal data are also complex and, in such scenarios, there are additional challenges even relating to the task of ascertaining which data are personal in the specific context in which they are collected and analysed. This is reflected in the following guidance examples from the UK Information Commissioners Office (ICO) on what is personal data:[133]

[131] Research by the Norwegian Consumer Council (NCC) in study #WatchOut, Analysis of smartwatches for children, October, 2017, https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf

[132] Study by Sophos, https://nakedsecurity.sophos.com/2017/10/19/kids-smartwatches-harbouring-major-security-flaws/

[133] UK Information Commissioners Office (ICO) webpage on 'What is personal data?'. Accessed at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

> *When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual.*
>
> *It is possible that the same information is personal data for one controller's purposes but is not personal data for the purposes of another controller.*

This is to say that, although the legal text of the GDPR provides significant coverage in relation to ensuring proper processing, there are still many steps for an organisation to take, as well as practical challenges to overcome, before data collection and processing activities are in line with the GDPR in practice.

To complement this point, there is presently a lack of previous evaluations as to whether EO (both data controllers and processors) are fully compliant for the types of products within study scope. Given how recent GDPR is, this isn't surprising; however, the ability to determine how effective the GDPR has been to date is crucial in determining if existing legislation is sufficient.

The research found several examples of dubious practices in respect of data collection by manufacturers, including many articles online about privacy not being respected, such as people's voices being recorded whilst they were using their internet-connected devices. However, whilst questionable data collection practices were more common pre-GDPR, given the risk of incurring fines from Data Protection Offices, such instances appear to be less common post-GDPR. However, there is only anecdotal evidence of this, as a systematic evaluation of the impact of GDPR overall, and more specifically in the area of its impacts on industrial products, especially internet-connected RE devices has not yet been carried out. The impact of GDPR will moreover take time to materialise, as legal cases and fines issued by DPOs gradually emerge and case law establishes precedents.

Sometimes, the user may not be aware of how their data is being used, by whom and for what purpose. Data collection can only be legitimate if there is transparency as regards the processing since the issue of fairness of processing is directly linked to transparency.

For example, the Smart TVs case study points out that some global manufacturers have revenue-sharing arrangements with third parties who collect and analyse data for example, on viewing habits both to personalise content and to be able to target advertising more effectively. Such a processing may be legitimate under the GDPR provided that all relevant obligations are complied with, including transparency and user consent, etc. However, stakeholders interviewed pointed out that users are often unaware that their viewing habits are being monitored.

There are also examples of smart products where data has been gathered without users' knowledge or consent. For example, there are well-publicised concerns regarding voice recordings made by certain models of **Smart TVs** in the middle of this decade without users' knowledge or permission and the data then being analysed to determine which topics of conversation users may be discussing whilst watching the TV, largely for advertising purposes.

In some instances, users may be informed about how their data will be used but the type of data being collected still raises privacy considerations. For example, a TV manufacturer acknowledged in their privacy policy in the small print that if users elected to use their voice recognition tool, then voice data could be recorded and data sold to third parties [134]. However, whilst the GDPR ensures that no such data can be collected without knowledge and an appropriate legal basis, there remain privacy considerations not only in relation to Smart TVs, but all sorts of new devices such as for **home automation systems** such as Alexa, Amazon Echo and Google Home.

Similarly, there are examples of smart toys such as the **Cayla doll** where voice recordings were made without users' consent. However, these examples are pre-GDPR. Such business practices would now

[134] https://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/

be illegal under EU law, and therefore, manufacturers should in principle be paying much greater attention to what types of data they are collecting, how it is being processed and stored, and whether consent has been obtained to collect the data and if the data has been collected in accordance with the GDPR's data minimisation rules. However, there is a lack of data or information on how extensively non-GDPR compliant data collection and processing is being undertaken.

Whilst consumers are now better protected in law, the problem of what constitutes proportionate personal data collection in the era of big data and the IoT is somewhat ambiguous, as has been attested in key literature.

Overall, the potential for data misuse by those collecting data from internet-connected RE devices, such as manufacturers, third-party service providers, etc. remains. A key change is that such activities are unlawful under the GDPR. Moreover, the legislation allows scope for large fines to be imposed. It is therefore uncertain if greater protection of personal data and privacy through the RED would address the problem of stopping illegitimate supplementary data collection by manufacturers and third parties.

In order to understand what types of data might legitimately be collected, it is worth providing a few selected examples as to why manufacturers collect data:

- Analysing product usage to feed into product redesign and engineering processes in future;
- Identifying commonalities and differences between users in terms of how they use products;
- To gather data about product performance to facilitate maintenance and servicing;
- Improving productivity and profitability;
- Better meeting the needs of their customers e.g. customisation of content and advertising, generating added value through big data analytics;

In terms of legitimate data collection, under the GDPR, firms must provide information to users and seek an appropriate legal basis to collect and process personal data, and this can be either through consent via a user interface or where the processing is necessary for the performance of a contract with a technology or service provider. In an IoT context, if access to a device/terminal equipment is made, then ePrivacy rules may be applicable, which and require consent. GDPR does not mandate consent in all cases, but the ePrivacy Directive does. However, a particular challenge in an IoT context is that interfaces to provide consent are less straight forward compared with for users in other more conventional internet contexts, such as visiting an e-commerce or a social media website via a browser, where interfaces can be designed prominently in a way that makes it easy for users to provide consent and / or to review and amend their privacy settings.

There is also some evidence that data misuse continues to be a problem, in spite of the GDPR, however, in the absence of evaluations of the impact of GDPR on industrial products, the extent to which is the case is difficult to ascertain. Nevertheless, experience from big tech suggests that there may be some grey areas where it is unclear what type of data may legitimately be collected and as to how far privacy should be protected. [135] There have been a number of widely-publicised examples of data misuse relating to Big Tech, such as the following examples from the above-mentioned Infolaw source:

- Twitter recently admitted that it "inadvertently" used the personal information of its users, which it collected on the pretext of security purposes, to enhance targeting of advertisements.
- Google is the subject of an investigation by the Irish data regulator, which has accused the search engine of "exploiting personal data without sufficient control or concern over data protection."

[135] https://www.infolaw.co.uk/newsletter/2019/11/what-is-data-misuse/

- Facebook has continued to face allegations of data privacy failures in connection which the sharing of user data with other tech firms, following on from the Cambridge Analytica scandal.

By analogy, it could well be the case that there are similar problems around delineating what types of data may legitimately be collected in a way that is GDPR-compliant by manufacturers in their capacity as data controllers and by third parties as data processors in respect of internet-connected RE. It has not been possible within the scope of an impact assessment on the RED to assess GDPR compliance systematically for connected RE devices.

The research also identified examples of data theft if users inadvertently provide their data as a result of fraud and scamming attempts in a phenomenon known as '**social engineering'**, when people are tricked into providing personal data. However, this is outside the scope of the RED, although it does heighten the importance of creating secure encrypted areas on devices that cannot be compromised by third-party software and apps. An example is that many mobile devices automatically save images and videos from WhatsApp and other messaging systems, including social media-transmitted images and videos, automatically to the images and videos areas of a mobile phone device. Secure encrypted parts of devices may possibly be needed.

In the absence of a clear user-interface to provide consent for some types of internet-connected RE products, are users aware that they have given their consent?

The research found that there are particular challenges in securing user consent due to the nature of the Internet of Things. Whereas it is easier to secure consent in a more traditional internet user interface (e.g. on a website), to change privacy settings, it is quite difficult to give consent for connected RE devices, because many simple RE devices lack a user interface. Even for complex equipment, user consent may be a one-off permission when the device is registered, without the user being clear how to update their privacy settings, for instance if the manufacturer changes these settings subsequent to them having given their initial consent. In practice, according to the desk research and some interviews, users remain confused about how to update consent.

An academic interviewed specialising in cybersecurity that has carried out research into the GDPR and the IoT commented that:

> *"The IoT is a complex ecosystem in which ubiquitous computing is all around us. Much more than cyber-physical systems. This raises issues as to how protection of privacy works in an IoT-enabled environment. Whilst the GDPR provides for data protection and privacy, designing an interface for giving consent in a shared IoT environment is not easy. The GDPR is structured around a web-based interface as the mechanism for developing a control system, and not for a dynamic IoT environment in which devices make autonomous and semi- autonomous decisions. IoT devices should be designed in a way that allows for some kind of interface through an app by changing the privacy settings".*

The challenge in ensuring compliance with the GDPR in an IoT context is also explored in recent literature, such as an EPSRC-funded research project examining issues related to giving and obtaining user consent online. [136] There are broader issues, such as the inter-relationship between the IoT and Artificial Intelligence (AI) that also impact the issue of obtaining user consent and complying with the data minimisation principle when connected RE devices may collect data and information autonomously, having asked for original consent only when the device was registered. An academic paper from 2019 [137] points out that:

[136] Meaningful Consent in the Digital Economy (MCDE)

[137] Prof. Dr. Lilian Mitrou, University of the Aegean, (2019). Data Protection, Artificial Intelligence and Cognitive Services, Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof" ?

> *"To achieve its full potential, the IoT needs to be combined with Artificial Intelligence (AI) and at the same time the impact of AI on every aspect of life will be multiplied and more sophisticated by its combination with the Internet of Things".*

There is a wide body of recent literature that raises issues around the application of the GDPR in an AI and IoT context. For instance, a further research paper [138]identifies the challenges that an "« ambient intelligence » era (involving the development of the IoT, with wide dissemination of RFID's, ubiquitous computing, "smart" objects and surveillance devices) raise from the points of view of "privacy" and "data protection". In conclusion, recent EU legislation has already strengthened data protection and privacy in terms of providing a legal framework for what data manufacturers and other economic operators may collect from users of internet-connected RE products. However, there are some grey areas in terms of implementing the GDPR in an IoT context in terms of managing the practical challenges for manufacturers, such as how to ensure that RE products are developed with a user interface, whereby users can express their privacy preferences. Nonetheless, the possibility of incurring fines under the GDPR ought to be having a positive effect in terms of manufacturers and other EO in global value chains taking such issues more seriously.

4.3 Stakeholders affected by security risks in connected radio equipment products

The nature and magnitude of security risks that affect users depends on factors such as:

- Who is using the product? How vulnerable are different types of consumers in terms of the risks associated with cybersecurity breaches in respect of their personal data and privacy/ or fraud?
- Where is the product going to be used? A smart thermostat in a home environment is potentially hackable, but has a relatively low impact of being hacked (as the user would notice and could take action to do something about it) whereas a smart thermostat being hacked in a nuclear power station, specific industrial or hospital environment could be highly dangerous.

Regarding users of internet-connected RE and wearable RE, a distinction is often made when identifying risks between professional product users and consumer usage. However, it was pointed out that in the case of consumer IoT, it is quite difficult to separate products intended for professional use, as opposed to consumer use. This would make it difficult to have a differentiated regulatory approach for instance between business-to-business ("B2B") and business-to-consumer ("B2C") IoT products.

The main priority for this study is on consumer IoT products and devices that fall under the RED's scope. In this vein, it is important to differentiate between the different levels of risk depending on the type of consumer using a particular RE product or wearable, i.e. between:

- **Consumers in general –** there are general concerns regarding the security of connected RE products and wearables, due to the fact that there are many low-quality, low-price products on the European market that are not cybersecure, and do not take data protection and privacy considerations into account. Moreover, even where consumers are aware about cybersecurity risks, the nature of risks evolves rapidly. Consumers may not therefore be aware of the most recent threats and vulnerabilities. Conversely, whilst many consumers want strengthened cybersecurity, not all consumers may be willing to add security measures if it means giving up the convenience of using the product.
- **Vulnerable consumers -** children and older people are often less cybersecurity-aware, and may not even be aware of the risks of using connected RE products and devices. Concerns regarding the need to strengthen the protection of users extends beyond conventional RE to the growing

[138] Privacy, Data protection, and the Unprecedented, Challenges of Ambient Intelligence, Dr Antoinette ROUVROY, Information Technology & Law Research Centre, University of Namur, Belgium

wearable devices market (smartwatches, FitBits), especially if these are intended to be used by children. Such devices allow parents to use an application on their smartphones to keep in touch with, and to track their children's location and may also contain a SIM-card, allowing children to connect to the Internet through mobile networks or Wi-Fi. This may pose safety risks for the child. Similar risks, as well as additional risks, such as children being recorded without the parents' permission, have been identified in respect of smart toys. [139]

4.4 Locational factors and risks

The location where connected RE products are being utilised affects the level of risk. A number of stakeholders interviewed made the point that under a risk-based approach, the level of cybersecurity risk, and the potential negative effects of a data breach will vary depending where a particular IoT device is being used. For example, a smart meter connected to a secured home network via a wireless router poses less risk than a smart meter installed in a critical infrastructure facility.

- The implications of this variance in the level of risk depending on the location where a product is intended to be used could be taken into consideration were a regulatory approach to be adopted. For example, if minimum baseline security requirements were to be set for all classes of RE, manufacturers could be required to carry out a risk assessment to assess different factors, such as: the type of connected RE product, whether there are particular device-level risks associated with its use, and where the product is likely to be used.
- The review of key literature presented in the background section provides examples of the risks associated with unauthorised access to geolocational information and data. Examples are smart watches targeted at children, and fitness app's used by adults, if the user works in a profession that could be a target for fraudsters or terrorists (e.g. military personnel). As the location of products/users is a type of data that can raise specific risks, then it is relevant to tackle the security of the processing of such data.

[139] Maras, M.-H. (2018). 4 ways "Internet of things" toys endanger children. *The Conversation* (May 10, 2018). https://theconversation.com/4-ways-internet-of-things-toys-endanger-children-94092.

5. Analysis of Policy Options, Impacts and CBA

This section provides an analysis of the Policy Options (Section 5.1), an assessment of the impacts associated with these policy options (Section 5.2) and a Cost-benefit analysis ("CBA") in Section 5.3.

5.1 Analysis of policy options

5.1.1 Strategic policy considerations – strengthening the security of internet-connected RE products

The findings from the problem definition and baseline assessment raise a number of strategic policy considerations regarding the best way forward to ensure that internet-connected RE incorporates adequate safeguards as regards sufficient data protection and privacy, and protection from fraud. The following questions informed the finalisation of the policy options, based on fine-tuning those defined by the European Commission in the Tender Specifications:

- To what extent does existing EU legislation, such as the GDPR, the ePrivacy Directive (soon to be ePrivacy Regulation) leave regulatory gaps as regards ensuring safeguards for data protection and privacy, and protection from fraud for internet-connected RE products and wearable RE?
- What is the optimal means of achieving strengthened resilience in respect of data protection and privacy, and safeguards to ensure protection from fraud for such products?
- Is a regulatory approach necessary through the activation of the two delegated acts already included in the Directive's essential requirements under Article 3(3)(e) and Article 3(3)(f)?
- Could a non-regulatory approach be an effective alternative to activating the delegated acts? What are the advantages and disadvantages?
- How should European regulators respond to the challenge of many products becoming increasingly complex, smart and internet-connected, meaning that they now fall within the RED's scope as they embed RE (as products increasingly incorporate Wi-FI and / or Bluetooth connectivity)?

5.1.2 Definition of policy options

A number of different policy options ("PO") were identified in the Tender Specifications. These reflect the impact assessment guidance in the Better Regulation guidelines, as they include a status quo option, non-regulatory and regulatory options. 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 in the Commission's inception impact assessment. [140] The options are outlined in the following box.

Table 5.1: Analysis of data collected by policy option

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).
Option 1 – Voluntary approach	Two different sub-options were considered:

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

Option	Description
Option 1.1 - Voluntary approach, such as industry self-regulation, and national governments promoting awareness of consumer IoT security.	• A situation in which industry implements existing EU legislation which protects personal data, the confidentiality of telecommunications, security and protection against fraud. Industry could then take the lead in self-regulating, for example, through the development of industry codes of conduct.
Option 1.2 – Voluntary measures to support the implementation of a regulatory approach.	• Non-mandatory accompanying measures to help manufacturers achieve compliance, such as awareness-raising measures about enhancing the security of internet-connected RE among manufacturers and consumers, and • The development of (voluntary) sectoral codes of practice on data protection and privacy (as per provisions of Art. 40/ 41 of the GDPR).
Option 2 - Adoption of a delegated act based on Article 3(3)(e).	• Internet-connected RE 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 RE would be required to incorporate certain features to ensure protection from fraud, and a tool to enhance the cybersecurity 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 (f).	• The requirements in Options 2 and 3 would have to be demonstrated for the purposes of market access. • This could 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 – Horizontal approach through development of a Mandatory Cybersecurity Act.	• A horizontal law would cover both wireless and wired products so as to avoid regulatory divergence between the two.

The possibility of maintaining the status quo and relying on the existing EU regulatory framework has been analysed in detail as part of consideration of the baseline situation (Option 0). As the legal framework – at least in respect of data protection and privacy – has evolved quite considerably in the past few years, this option was given serious consideration.

Whilst the options above were those defined in the ToR, additional possibilities suggested by stakeholders have been considered. Regarding the possibility of a voluntary approach (Option 1), we have distinguished between an approach centred purely on self-regulation, either led by industry, government or the two working together, as opposed to one in which voluntary initiatives could support the effective implementation of a regulatory approach, such as the development of guidance for industry and users of internet-connected RE support the implementation of regulation.

The rationale for defining these two sub-options is that several stakeholders stated that a regulatory approach would only be effective if supported by accompanying measures, such as awareness-raising among manufacturers and other EO in global value chains (GVCs), 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 RE.

The relative advantages and disadvantages of a regulatory approach (Options 2, 3 and 4) have also been analysed, in which either one or both delegated acts in study scope were to be activated. This would require minimum baseline security requirements to be implemented alongside existing applicable EU regulations relating to data protection and privacy.

As regards Option 5, the scope to adopt a horizontal piece of legislation on cybersecurity in a broader sense, some stakeholders, especially industry associations and individual manufacturers responding to the targeted survey, supported consideration of a horizontal mandatory piece of legislation in future which could cover all industrial products.

This was put forward as a means of ensuring that both wireless and wired products were covered rather than having a differentiated legislative approach to safeguarding data protection and privacy and ensuring improved protection from fraud through the RED, which could lead to similar adaptation of other industrial product legislation over time. Whilst this could only realistically be achieved over a medium-term timeframe, as it is considered a viable approach – and preferable in the views of some stakeholders to incorporate such requirements in individual pieces of industrial product legislation, it has been considered as a separate option.

The findings in relation to the examination of the different policy options are based on a combination of desk research and interviews.

5.1.3 Policy Option 0 - Status quo: reliance on existing EU legislation

Policy Option 0 would involve a continuation of the status quo, i.e. a situation in which existing EU legislation would be relied upon to achieve key EU policy and regulatory objectives.

The current situation is that manufacturers of internet-connected radio equipment and other EO integrated within Global Value Chains (GVCs) are not subject to essential requirements under the RED either relating to data protection and privacy, or protection from fraud, as a condition of market access. Therefore, products may legally be placed on the market even if they are insecure, at least as far as the RED's scope is concerned.

However, whilst there are no obligations under the RED, other EU legislation regarding data protection and privacy is applicable. A detailed legal mapping of the baseline situation was provided in Section 3.3 - Analysis of existing EU legislation and regulatory gaps. The overall findings from the assessment as to how effective existing legislation is, and whether there remain any regulatory gaps are now presented:

5.1.3.1 Data protection and privacy

The EU legal framework already partially addresses data protection and privacy through the GDPR Regulation **(EU) 2016/679**, and the **ePrivacy Directive 2002/58/EC (ePD).** The latter is currently under revision to align it with the GDPR through the **proposed ePrivacy Regulation** [141] , to strengthen privacy for individuals and businesses in the transmission of electronic communications data.

Moreover, a series of clear definitions are provided in the GDPR in respect of key concepts such as data protection, privacy, data controller, data processor, consent, data subject etc. These already help to provide protection for users of internet-connected RE by providing a clear legal framework.

A number of Articles in the GDPR are especially relevant in addressing the issue of ensuring data protection in internet-connected RE, namely: **Art. 24 (technical and organisational measures); Art. 25 (data protection by design and default); Art. 35 (Data Protection Impact Assessments); Art. 40 (voluntary codes of conduct on data protection and privacy at a sectoral level); and Art. 43 (the role of accreditation bodies)**.

There are **evaluability challenges** in assessing how far the existing body of EU legislation is fit for purpose as regards ensuring adequate safeguards for data protection and privacy in internet-connected RE products. Much of the most relevant EU legislation is relatively new, and therefore its

[141] COM/2017/010 final - 2017/03 (COD) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

effectiveness has not yet been evaluated. For example:

- The GDPR only came into effect on 28th May 2018 and has not yet been evaluated.
- The CSA only became law in July 2019 and no product-specific certification schemes have yet been developed)
- Whilst the e-Privacy Directive has been in place since 2002, the proposed ePrivacy Regulation to align the e-PD with the GDPR, and to strengthen privacy protection has undergone a series of proposed revisions and the final legal text has not yet been agreed.

As regards **regulatory gaps** in the EU legal framework in which manufacturers of internet-connected RE operate, the GDPR leaves some gaps. Specifically:

- Fines may be issued under the GDPR, but as there are no equivalent rules relating to data protection and privacy under industrial product legislation, such as the RED (for wireless products), only 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. According to national authorities and MSAs interviewed, the fact that MSAs are unable to remove unsecure products from the market, either the RED, or other EU legislation, leaves a gap[142.]
- In the absence of any enforcement powers under the RED or any other EU legislation to allow internet-connected RE products to be removed from the market, the Cayla doll example was cited by interviewees as an example of a product that despite known flaws, cannot not legally be removed from the European market.
- Indeed, some Member States (MS) have instead had to use different pieces of national legislation to find alternative ways of 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.
- Although fines can be issued under the GDPR, which may serve as a deterrent, products cannot be removed other than through recourse to national legislation, which consists of an obscure patchwork of legislation[143]. This means that there is a risk that the internal market's effectiveness as regards the free circulation of internet-connected RE products could be undermined, since there are no legal enforcement powers presently to remove products from the market.
- Moreover, some MS authorities have requested in the past 12-24 months that the European Commission should actively investigate the possibility of activating the DAs to prevent the emergence of divergent national laws concerning the security of internet-connected RE, data protection and privacy and protection from fraud.

The GDPR sets out specific obligations for data controllers and processors as regards the collection and processing of personal data, but if a manufacturer is not intending to collect such data, there is no obligation to take security into account.

Software developers and technology providers providing services that gather and process personal data via the internet and exploit such data for big data analytics purposes are already subject to the GDPR. If software developers and technology providers provide products/services that personal data and then use/exploit the data themselves, they automatically fall under the GDPR's scope. They remain outside the GDPR's scope if they only design products and services, but do not take part in any

[142] Whilst some national authorities were able to remove the product, they had to rely on national legislation rather than EU legislation to do so. This may risk undermining the effective implementation of a single market in RE.

[143] In the case of the Cayla doll, national authorities and MSAs 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.

actual data processing. This is a regulatory gap as in such a situation, there is instead a reliance on the product design engineers and subsequently the manufacturer (which may include suppliers and Original Equipment Manufacturers to implement security by design and default on a voluntary basis.

Moreover, anecdotal evidence (which would need to be verified in an evaluation of the GDPR) suggests that not all manufacturers and service providers are aware that they have any legal responsibilities under the GDPR, nor are clear as to how far their responsibilities extend across the value chain, which may be complex and global as regards how data is collected, processed and used by third parties.

More positively, the GDPR has already made a positive impact by strengthening attention to data protection and privacy, for instance by making most manufacturers (especially medium and large-sized) aware that if they intended collecting or processing personal data, they are data controllers and therefore have legal obligations to implement data protection by design and default (Art. 25) and to implement appropriate organisational and technical measures (Art. 24).

The evidence gathered through the product case studies found that data protection by design and default is being strengthened through the **integration of security by design principles into the design, engineering and manufacturing processes by manufacturers of internet-connected RE**. Moreover, GDPR was seen by some manufacturers interviewed as having promoted changes to business practices and to documenting these so that it has become more transparent from a business process mapping perspective how a given manufacturer has given consideration to data protection by design and default principles from the outset.

A further area where more evaluative assessment is needed in future is the **level of compliance with Art. 25** by manufacturers selling internet-connected RE in the European market, as regards whether they are European or global. The extent of monitoring and enforcement of this Article by Data Protection Authorities (DPAs) is also difficult to ascertain at this relatively early stage in implementation. However, the research suggests that to date there have been only three legal cases relating to Art. 25. None of these related to manufacturers of connected RE or broader industrial products.

It is likely to take time for the GDPR's full impact to be manifested, as for instance, the potential deterrent effect on manufacturers of internet-connected RE products as regards the risks of being non-compliance in respect of Art. 25 (data protection by design and default) will be incremental, as it will take time for a sufficient critical mass of enforcement actions and the outcomes of legal cases to be available. Moreover, it will take time before there is publicity regarding any fines issued and associated case law has an impact on manufacturers' behaviours. Nevertheless, regardless, some manufacturers interviewed attested to high levels of awareness about GDPR and the need to document business processes more carefully, including how data protection and privacy issues have been managed (see, for example, the laptops and smart toys case studies in Annex 8).

Many **users of internet-connected RE appear to be unaware as to what data is being collected automatically** by such products, devices and equipment, and as to how this data is being used by manufacturers (data controllers), third parties (data processors) and service providers (data processors). Whilst there is a legal requirement for consent to be obtained before such data can be collected or processed, this does not necessarily mean that the situation is clear from a user perspective. The desk research and interviews also pointed to there being challenges in securing consent in a consumer IoT context, as designing interfaces through which consent can be obtained is not always straight forward.

A finding from one of the product case studies (e.g. Smart TVs case study in standalone annex) found that although the law is clear, there is a degree of tension between the principle of data minimisation in GDPR, and the evolution of big data driven business models in an IoT context, with extensive data being gathered either fully or semi-autonomously.

The literature review presented in Section 3.3.2 (Data protection and privacy in the context of internet connected RE) suggests that whilst the GDPR sets out relevant rules to ensure data protection and privacy, there has not been an evaluation of the GDPR as yet, and specifically of whether there are practical difficulties and challenges in implementing the GDPR effectively in an IoT era.

For instance, there appear to be a **lack of cooperation mechanisms between national DPAs responsible for the GDPR, and national authorities and market surveillance authorities (MSAs) responsible for monitoring and enforcement of the RED**. Some stakeholders interviewed commented that there is a disconnect between the GDPR, whose implementation is driven by lawyers and data protection officers within firms, and product engineers and product compliance managers used to dealing with the essential requirements for EO set out in industrial product legislation and in harmonised technical standards. It was noted that the two speak different languages and have a different understanding of the challenges and reality of applying GDPR principles in an IoT context.

However, it was made clear by the European Commission's DG JUST that the **GDPR is fully applicable in an IoT context.** Some stakeholders therefore argue that there is no need for specific legislation to be applied to IoT data protection rules that are already in the GDPR. However, other stakeholders – especially consumer associations and national authorities - are of the view that there are weaknesses in relying on the GDPR alone as the rules need to be implemented in an industrial products context, and recognise the specific challenges of ensuring data protection in internet-connected RE products and wearables in an IoT context. They pointed to the loophole that not all product designers and manufacturers fall explicitly within the GDPR's scope if they are not categorised as a data controller as they do not collect personal data.

Some stakeholders (mainly industry associations and large manufacturers) argued that the GDPR was already sufficient in ensuring data protection, as data controllers and processors could potentially be subject to large fines if they do not comply with the GDPR's requirements, including *inter alia*, adequate consideration of technical and organisational measures to ensure data protection (Art. 24), and the obligation to consider data protection by design and default (Art. 25).

However, this was seen by other stakeholders as being insufficient, as **GDPR compliance is not a market access requirement under the NLF common approach (unlike the RED)**. Under Article 58 GDPR, DPAs have many powers at their disposal, including the power to impose a temporary or definitive limitation, including a ban on processing. However, under the GDPR, DPAs do not have the power to withdraw products from the market, even if evidence is identified of inadequate data protection and privacy.

Some feedback was received on the relative effectiveness of the **e-PD** in protecting users of internet-connected RE products. Whilst the Directive was seen as useful in protecting users' data, it concerns the processing of personal data and protection of privacy in electronic communications, including e-commerce transactions. It does not presently provide protection in respect of device-level security i.e. ensuring that internet-connected RE (especially consumer IoT devices but not limited to) integrate basic cybersecurity functionality into their design from the outset, and that this is ensured prior to such products being placed on the market.

Feedback was also received in respect of the extent to which the **Cybersecurity Act (CSA)** might make a difference, although this is focused on cybersecurity in a broader sense, rather than specifically on the security of internet-connected RE with specific reference to data protection and privacy and protection from fraud.

- Whilst the CSA may have a positive influence on market behaviours as a result of industry engaging in the development and rolling out of (voluntary) ICT security certification schemes, since the scheme is non-mandatory, it may not achieve the Commission's regulatory objectives of strengthening the security of internet-connected RE in the above-mentioned areas.

- Although some stakeholders perceived that the CSA is more focused on product groups and sub-sectors in the Business to Business (B2B) arena than in Business to Consumers (B2C), discussions with ENISA found that strengthening the cybersecurity of consumer IoT will be among the first areas in which a product certification scheme will be developed. This could also contribute to improving data protection and privacy and protection from fraud, as preventing online device penetration would resolve many of the problems.
- However, a weakness of relying on the CSA to achieve policy and regulatory objectives noted by interviewees is that it is only a voluntary initiative will be rolled out gradually across different product groups. Nevertheless, the CSA was regarded as providing a viable mechanism to strengthen attention to security in the design of internet-connected RE, at least by some industry associations and manufacturers.

5.1.3.2 Safeguards to ensure protection from fraud

In contrast to data protection and privacy, there was found to be a lack of EU legislation to address protection from fraud, an exception being the Non-Cash Payments Directive (Directive (EU) 2019/713). This is not however relevant to industrial products, but does provide some useful concepts as regards fraud prevention. Whilst this Directive provides a useful starting point in terms of defining fraud, it is concerned with tackling fraud in connection with non-cash means of payment, such as cryptojacking. It does not address the need to strengthen security in an industrial product context i.e. ensuring security prior to their placement on the market.

Further issues relating to protection from fraud are explored under Policy Option 3, activating Article 3(3)(f).

5.1.3.3 Cybersecurity protection in a broader sense

The **Cybersecurity Act (CSA)** is a voluntary, certification-based approach to addressing security issues across different ICT sectors entered into force on 27 June 2019. The CSA is likely to include measures to develop baseline security requirements which could help to prevent data breaches, and thereby strengthen safeguards for data protection and privacy, and protection from fraud. However, the CSA is generally being implemented through the development of product-specific certification schemes, under the overall coordination of ENISA but with inputs from industry .

Whilst some certification schemes could be relevant, such as a proposed scheme covering consumer IoT products, these are currently under development, and none have been finalised. In reviewing existing EU legislation, a key issue investigated was whether the activation of either one or both of the two delegated acts foreseen in the RED under Articles 3(3)(e) and 3(3)(f) relating to i) data protection and privacy and ii) safeguards to ensure protection from fraud would be complementary to, or duplicative with existing EU legislation.

5.1.3.4 Findings – Policy Option 0 – Status quo

Overall, the status quo option is feasible in that at least in the areas of data protection and privacy, there are already legal requirements for manufacturers that afford some degree of protection in the GDPR for users of internet-connected RE and wearables. However, arguably there is insufficient regulatory protection, as products that do not provide basic security protection to ensure safeguards for users' data can remain on the European market.

- Whilst fines can be issued under the GDPR by national DPOs, it is not possible for MSAs – who often have a better understanding of technical issues relating to the security of internet-connected RE products to either test such products for compliance with any security requirements or to remove them from the market.

- A weakness in the existing essential requirements in the RED (in common with other industrial product legislation) is that there is no explicit connection between product safety (already in the essential requirements) and security, despite inter-linkages between the two mentioned by a number of stakeholders (e.g. consumer associations, also some industry associations focused on cybersecurity).

If the Commission were however to proceed with the 'status quo' option, this would only be effective under certain caveats, such as:

- Strengthening the evidence base as regards the impact of the GDPR on internet-connected RE and wearables from a data protection and privacy perspective (see recommendations – Section 6.2.1).
- Active enforcement by Data Protection Authorities of the existing provisions in the GDPR, for instance Art. 24 (organisational and technical measures to prevent users' data from being compromised), Art. 25 (data protection by design and default) and Art. 35 (data protection impact assessments in instances where data is particularly sensitive).
- As there have been few legal cases in respect of these Articles, it is difficult to say how effective the GDPR has been in fostering behavioural changes among manufacturers and economic operators to take the issues concerned more seriously in the design, engineering and manufacturing of the RE products in study scope.
- The pace of roll-out of the CSA, which is a legal act, but which relies on a voluntary approach with active industry engagement would need to be accelerated. Currently, the CSA has only just come into force, and it is too early to assess whether this is likely to be effective in addressing the security of internet-connected RE products and wearables from a data protection/ privacy / fraud perspective.
- Irrespective, the certification schemes developed through the CSA could be useful to achieving key EU policy objectives, irrespective as to whether the Commission adopts Option 0, Option 1 (as the CSA certification schemes are voluntary) or Options 2-4 (as a regulatory approach could benefit from building on existing standards and certification schemes).

5.1.4 Policy Option 1 – A voluntary approach

Policy Option 1 relates to the possibility of adopting a voluntary approach to addressing the concerns of consumer associations, national authorities and MSAs (as well as some EO) relating to the cybersecurity of connected RE. The desk research and interview feedback suggested a distinction between a purely voluntary approach, and voluntary measures to help implement EU legislation. The two different sub-options defined are therefore as follows:

- Option 1.1 - Voluntary approach
  - Approaches characterised by industry-led, self-regulation; and
  - Development and publication of good practice guides and industry codes of conduct relating to consumer IoT security.
- Option 1.2 - Implementation of a regulatory approach, but supported by voluntary measures and non-mandatory additional (optional) requirements in EU legislation:
  - The use of non-mandatory initiatives, such as EU-level codes of conduct and awareness-raising measures to help manufacturers to achieve compliance.
  - The incorporation of non-mandatory elements into EU legislation. For example, there are (voluntary) certification schemes under the CSA, even though the latter is a legal act. Additionally, there is scope under Art. 40 of GDPR for voluntary codes of conduct to be developed on a sectoral basis, which are non-mandatory.

The findings to date are now outlined.

5.1.4.1 Option 1.1 - Voluntary approach.

The findings relating to the first sub-option are first outlined. This relates to a voluntary approach either through industry-led self-regulation or involving public sector-led initiatives to raise awareness about cybersecurity in RE products and to promote changes in the behaviour of market participants in terms of how they treat cybersecurity in the consumer IoT product design process. The findings from the desk research were that:

- A number of EU and national stakeholders have developed good practice guidance and codes of conduct relating to consumer IoT, such as DCMS' Code of Practice for Consumer IoT Security[144] *(presented in Section 3.1.5 - National developments)*. Furthermore, various industry associations such as Digital Europe, have developed guidance on different aspects of IoT device cybersecurity. These could feed into the **emerging development of technical solutions and certification schemes.**
- ENISA has also developed **baseline security requirements for IoT products.** [145] While the focus of the original guidance document was on the specific risks posed when connected IoT products are installed in particular locations, such as in critical infrastructures, the general principles relating to cybersecurity in the design of consumer IoT devices have wider applicability and relevance.
- The general principles relating to security by design and default[146] highlighted in the documents and recommendations made on baseline security requirements by organisations such as ENISA and NIST, as well as guidance on consumer IoT security developed by DCMS and others, provide a starting point from which **more detailed technical solutions for connected RE 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.
- **The codes of conduct, guidance and recommendations on IoT security and on best practices for IoT manufacturers that have been developed to date are relatively recent.** The guidance documents date from 2017 and 2018 (ENISA), 2018 (DCMS) and 2019 (NIST). The guidance stresses many of the same elements, but to varying degrees of technical detail. Since the guidance and industry codes were produced relatively recently, there was no feedback on how effective the guidance has been. In the UK, there was only limited evidence of formal engagement and adoption of the voluntary code of practice.
- Although it is too early to assess the impact of such guidance and recommendations on the behaviour and practices adopted by manufacturers and other EO, key principles relating to security by design and default emphasised in these documents remain relevant. They influenced the development of the ETSI Technical Standard on consumer IoT security (2019).
- 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, **they may be insufficient by themselves to drive change sufficiently quickly to address the concerns of consumers, regulators and market surveillance and enforcement authorities.** This is particularly

[144] UK Department for Digital, Culture, Media and Sport. (2018). Code of Practice for Consumer IoT Security. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

[145] 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.

[146] Security by design and default principles also underpinned the development by ETSI of the world's first globally-applicable standard for consumer IoT security. The ETSI Technical Committee on Cybersecurity published TS 103 645 on 19 February 2019.

the case, given the growing ubiquity of IoT consumer devices.

- The UK provides an example where initially DCMS decided that a voluntary approach would be preferable. Accordingly, it developed a code of practice for industry on consumer IoT security, alongside guidance for consumers to raise awareness of the problem. However, it has subsequently decided a year later that **a regulatory approach may still be needed.** It launched a public consultation in June 2019[147] to review the relative advantages and disadvantages of a voluntary and mandatory approach to addressing consumer IoT security.

The interview programme findings were as follows:

- **A number of stakeholders were in favour of pursuing an industry-led, but voluntary approach.** This was to avoid any additional new regulations, which some viewed as unnecessary, since the CSA has only just come into effect. The CSA could therefore provide an alternative (voluntary) mechanism to achieve higher levels of cybersecurity. The stakeholders that supported this approach included: major industry associations (especially manufacturers of household appliances and electrical equipment) and some individual companies.
- However, other stakeholders, such as individual manufacturers, as well as cybersecurity associations and firms, disagreed and advocated for a regulatory approach since this would **provide greater legal certainty for firms and consumers**.

Box 5.1: Case study - Voluntary codes of practice to strengthen the security of internet-connected RE and wearables.

Rationale for the development of voluntary codes of practice and other frameworks relating to strengthening the security of internet-connected RE. The problem of security vulnerabilities in consumer IoT devices has been recognised by many stakeholders, including consumer associations, MSAs, and some industry groups and individual manufacturers. In the absence of mandatory requirements relating to IoT security in internet-connected RE devices, some national authorities and industry associations have been exploring how voluntary codes of practice and other good practice tools, could help to address the problem of the lack of sufficient attention to the embedding of security by design and default principles into consumer IoT products. Such guidance has the potential to raise awareness among manufacturers and industry more broadly regarding the need to ensure that common sense principles are integrated into product R&D&I processes from the outset.

Examples of those that have been working on different guidance documents are: DCMS in the UK, and the IoT Security Foundation [IoTSF]. At European level, there are also examples of similar initiatives, such as the publishing of studies and guidance on security by design and default by the European Consumer Associations. ENISA has also been examining how to strengthen IoT security, both through its work on the Cybersecurity Act, adopted in 2019, and on ensuring IoT security in user environments that pose additional risks, such as protecting critical infrastructures[148]. In common with the ETSI standard, the subject of another case study, the focus of several initiatives is on developing good practice principles and recommendations on consumer IoT security crucial to ensure functionality.

Description of technical solution(s)

Whilst there are a wide range of initiatives, this case study focuses on:

1. **ENISA's baseline security requirements,** as set out in Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures[149] (November 2017).

[147] DCMS unfortunately has not responded to requests for an interview regarding the as yet unpublished consultation outcomes.

[148] ENISA. (2017). Defining and securing the Internet of Things: ENISA publishes a study on how to face cyber threats in critical information infrastructures. https://www.enisa.europa.eu/news/enisa-news/defining-and-securing-the-internet-of-things.

[149] 149 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

2. The **IoT Security Compliance Framework** was published in December 2016 by the IoT Security Foundation [IoTSF], and updated to reflect the DCMS code of practice below.
3. The **Industry Code of Practice on Security by Design** (October 2018) developed by DCMS in the UK.

The key features of selected examples of (minimum) baseline security requirements, good practice guides and industry codes of practice (relating to security by design and default) are now described, and any lessons learned from their usage to date are then considered.

Although the study title implies a focus on security risks linked to the use of IoT products in critical infrastructure, **ENISA's baseline security requirements** cover IoT security in a broader context. The report "serves as a reference point in this field and as a foundation for relevant forthcoming initiatives and developments" by ENISA. Some aspects of the baseline security requirements are relevant to ensuring cybersecurity of IoT devices that could potentially be relevant since they would fall within the RED's scope. Examples are in the field of authentication:

- GP-TM-21: Design the authentication and authorisation schemes (unique per device) based on the system-level threat models.
- GP-TM-22: Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.
- GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., on top of certificates.
- GP-TM-24: Authentication credentials shall be salted, hashed and/or encrypted.
- GP-TM-25: Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices.
- GP-TM-26: Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.

There are also elements in the baseline security requirements that are relevant to Article 3(3)(e) and the possible Delegated Act in the RED, notably the principles in the ENISA guidance pertaining to **compliance with data protection requirements set out in the GDPR.**

There are also some further references in the ENISA baseline requirements to data security and privacy under the heading of "Access Control - Physical and Environmental security", notably:

- GP-TM-29: Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy.
- GP-TM-30: Ensure a context-based security and privacy that reflects different levels of importance.

Under the heading "Secure and trusted communications", there are further references to ensuring data privacy and confidentiality, including the important role played by the encryption of data:

- GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud.
- GP-TM-39: Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.

Overall, ENISA's baseline security requirements have been influential in setting the agenda for other developments to strengthen consumer IoT security, and many of the detailed principles in the ENISA guidance have been incorporated into more recent developments, such as the development of the ETSI standard and the industry code of practice by DCMS. The latter focus however on higher-level basic requirements, whereas the ENISA guidance already provides more detailed principles. The other initiatives in focus are now examined:

The **IoT Security Compliance Framework** is targeted at the consumer IoT and Smart Home markets. It consists of a comprehensive checklist which provides guidance for different stakeholders in the value chain, such as Device Manufacturers, IoT Service Providers, Mobile Application Developers and Retailers. The framework is based on taking economic operators through an assurance process, gathering evidence in a structured process and conforming to good practices and applicable standards. The Compliance Framework is written It aims to translate high-level guidance on IoT security into operational practices. It is comprised of two parts:

- **Part 1 – A set of Best Practice Guides.** These are designed for use by all departments within a given enterprise and define what steps need to be taken to incorporate adequate cybersecurity into products, services and operations.
- **Part 2 - The Compliance Framework.** This consists of a checklist of all the elements that managers in EO need to ensure that when a product is developed and put on the market, it is compatible with security by design and default principles both at the point of being put on the market, and throughout its entire life-cycle post-placement to design it securely and to keep it secure. The framework has been developed for all actors in the supply chain for IoT products and services, from the initial provider of technology components through to retailers and service providers. The guidelines are drafted in a way that is meant to apply both internally and to the supplier base.

The UK's Department for Digital, Culture, Media and Sport (DCMS) published a **Code of Practice for Consumer IoT Security** in October 2018. The DCMS guidelines are targeted at 1) Device Manufacturers 2) IoT Service Providers 3) Mobile Application Developers and 4) Retailers selling internet-connected RE products and associated services to consumers.

This stressed Security by Design and Default in some detail and was accompanied by a Technical Report on Security by Design: Improving the cyber security of consumer Internet of Things (products and associated services). The CoP stresses the importance of support all parties involved in the development, manufacturing and retail of consumer IoT with a set of guidelines to ensure that products are secure by design. The code consists of thirteen outcome-focused guidelines, which draw on good practices in IoT security. Of the thirteen, the first three guidelines have been prioritised since **action on default passwords, vulnerability disclosure** and **security updates** was identified as bringing about the largest security benefits.

Potential effectiveness and utility of the technical solution(s) and possible limitations:

- The **ENISA guidelines on baseline IoT security requirements** provide detailed guidance on how to integrate security by design and default considerations into product design and usage. They place an emphasis on the additional set of risks that emanates from using IoT products and devices depending on the location where these are being used. Certain environments, such as critical infrastructures, are considered high-risk. This provides an interesting example, as several stakeholders interviewed pointed to the need to look beyond device-level risks (within the RED's scope), and also to assess the risks more holistically, for example, considering products are being used, and the network risks.
- The **Compliance Framework focuses on the product life-cycle.** A challenge in this regard - as with the ETSI TS on consumer IoT security (ETSI TS 103 645) - is that the RED's scope addresses product safety leading up to placement on the market. If the DA were to be activated, then whilst this would ensure that the links between product security and safety were covered in the essential requirements, it would not fully address the product lifecycle approach to ensuring security advocated by some stakeholders. Some stakeholders, including some MSAs and industry associations, therefore advocated an approach across industrial product legislation through the possible introduction of a horizontal regulation on cybersecurity covering all industrial product legislation.
- The **IoT Security Compliance Framework** and **Industry Code of Practice on Security by Design** are both helpful, and share similarities with some of the basic common-sense principles integrated into the umbrella ETSI TS on consumer IoT security. However, the fact that they are non-mandatory means that there is no regulatory mechanism to ensure that manufacturers follow security by design and default principles. Therefore, whilst useful in raising awareness about these principles, neither of these initiatives, by themselves, maybe adequate to bring about changes to manufacturing practices in terms of engineering out security vulnerabilities from the outset of the design phase.

Lessons learned:

- The ENISA guidance on baseline security requirements provides a useful model that could service to inform the development of detailed technical requirements at the product level.
- Whilst the DCMS Code of Practice provides clear, top-level requirements that need to be met, as the IoTSF points out *"translating these into practice can be technically complex".* Therefore, a lesson learned is that developing, publishing and disseminating good practice guidance by itself is insufficient to bring about positive changes in the security of internet-connected RE (especially consumer IoT devices and products, where products appear to be most prevalent) without detailed technical solutions at the product level.
- The IoT Security Compliance Framework provides an example of a more detailed framework aimed at those involved in ensuring product and device security. This suggests a general need for codes of practice setting out high-level minimum security requirements based on a set of principles to be accompanied by practical and operational guidance.
- The focus in the IoT Security Compliance Framework on ensuring that security principles are communicated throughout the supply chain to strengthen trust between different EO can be seen as a good practice. However, as noted under "possible limitations", the RED focuses on the period leading up to the placement on the market rather than a product lifecycle approach, although arguably designing products to be secure by design and default ought to ensure that vulnerabilities post-placement on the market are kept to a minimum.
- Further good practices are that the Code of Practice for Consumer IoT Security was developed in conjunction with the National Cyber Security Centre (NCSC), thereby ensuring that excellence in IoT security was tapped into. Secondly, the organisation of a 6 months consultation on the draft Code, and active stakeholder engagement with industry, consumer associations and academia, can be seen as a further good practice.

Sources: Desk research, review of the DCMS Code of Conduct and the IoT Security Compliance Framework (IOTSF), interviews with stakeholders familiar with the guidance.

5.1.4.2 Option 1.2 – Voluntary measures to support the implementation of a regulatory approach.

Whereas Option 1.1 related to a purely voluntary approach, a number of stakeholders pointed out that the implementation of a regulatory approach could be supported by a combination of voluntary measures, as part of an integrated approach to improve the effectiveness of possible future legislation. This could consist of voluntary measures and initiatives, such as:

- The **development of EU and national codes of conduct** aiming to promote and disseminate good practices in security by design and default (as described under Option 1.1, but used in conjunction with a regulatory approach under Option 1.2). These would help EO to achieve compliance under a regulatory approach;
- **Sharing good practices in respect of possible technical solutions relevant to strengthening consumer IoT security.** These could be shared between the ESOs, national authorities, MSAs, testing bodies, notified bodies and industry. This would be useful in respect of the future development of harmonised technical standards, were a regulatory approach to be adopted;
- **Ensuring that there is capacity-building to strengthen capacity among ESOs, testing bodies and notified bodies to check connected RE products from a security perspective.** The feedback from several stakeholders suggested that whilst there is some expertise in testing products against security standards, further capacity-building would be needed to ensure for instance that:
    - Standards organisations are able to develop robust technical standards in the field of the security of internet-connected RE, since they have previously focused on developing harmonised product safety standards;
    - MSAs and testing bodies should receive training and capacity-building so that they are able to provide the necessary technical testing services to check RE products to ensure that they have

basic security functionality[150]. Many testing houses have only limited – if any - experience in testing the security of internet-connected RE.

- **Awareness-raising measures** to draw manufacturers' attention to the importance of strengthening the security of internet-connected RE in consumer IoT and of integrating security by design and default principles into the design stage and into manufacturing processes, including the procurement of components within GVCs.

According to several stakeholders, such measures could play a role in improving the effective implementation of possible future legislation. The above-mentioned different types of measures could be appropriate since some stakeholders (especially national authorities, MSAs and cybersecurity industry associations) said that awareness levels among manufacturers regarding basic security functionality of internet-connected RE is low. Whilst recognising that many companies have made progress, there remains a perception that some market participants have not yet embraced a culture of security by design and default, or integrated security considerations into product safety throughout the product lifecycle.

It is also important to note that there are **non-mandatory requirements embedded within some existing EU legislation.** This demonstrates that implementing a regulatory approach may sometimes benefit from additional voluntary measures in parallel. Examples are provided below:

- Even though the CSA is a legal act, it is being implemented through (voluntary) certification schemes coordinated by ENISA, which are being developed on a product-by-product basis. The CSA is also relevant to Option 0, in that it is part of the existing legal framework. However, it is especially relevant to Option 1.1, since the involvement of industry in certification schemes on a product by product basis is voluntary.
- Additionally, there is scope under Art. 40 of the GDPR for voluntary codes of conduct to be developed on a sectoral basis. These are non-mandatory and participation is at the discretion of the sector concerned, depending on the level of interest among industry.
- Extensive feedback was received in respect of the recent adoption of the Cybersecurity Act (CSA), which is a mechanism for strengthening cybersecurity that relies upon (voluntary) certification schemes, which are developed under the overall coordination of ENISA.
- Some industry associations and manufacturers saw there as being advantages in expanding the existing certification schemes under the CSA, before even considering recourse to a voluntary approach since the CSA was only adopted in June 2019, and the process of rolling out the scheme to different product groups will take considerable time, since it requires engagement with product-specific industry groupings, and technical work to develop certification approaches.
- The GDPR provides for a toolbox to facilitate the proper application of the Regulation. For example, **Article 40(2) of the GDPR makes provision for the development of voluntary sectoral codes of conduct.** These Codes may cover different aspects of data protection, including the need to ensure fair and transparent processing, the collection of personal data, technical and organisational measures to ensure data protection by design and by default and security measures, and personal data breach notification.
- The **European Data Protection Board** has developed *Guidelines1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* [151]*.* These could be a useful model as to how to engage with different sectors. Further details about these codes are provided in the following box.

[150] Simple testing might involve checking that a consumer IoT product does not use a default username and password, has data encryption and authentication capabilities, etc.

[151] European Data Protection Board, Guidelines on Sectoral Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Guidelines on sectoral codes under the GDPR - 1/January 2019. Pg. 6 , https://edpb.europa.eu/sites/edpb/files/consultation/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf

Box 5.2: Sectoral Codes under the GDPR, Art. 40(2).

Example of voluntary mechanism within a mandatory piece of legislation: The role of Trade Associations and Sectoral Bodies in drawing up Provision is made under the GDPR for the drawing up of Voluntary codes on data protection under Art. 40(2) of the GDPR.

Relevance: addresses data protection and privacy, data breaches, etc.

Description: GDPR sectoral codes are voluntary tools which set out specific data protection rules for categories of data controllers and processors. These can be *"a useful and effective accountability tool, providing a detailed description of what is the most appropriate, legal and ethical set of behaviours of a sector. From a data protection viewpoint, codes can therefore operate as a rulebook for controllers and processors who design and implement GDPR-compliant data processing activities which give operational meaning to the principles of data protection set out in European and National law".*

As provided for in the non-exhaustive list contained in Article 40(2) of the GDPR, codes of conduct may notably cover topics such as:

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection of personal data; the pseudonymisation of personal data;
- the information provided to individuals and the exercise of individuals' rights;
- the information provided to and the protection of children (including mechanisms for obtaining parental consent);
- technical and organisational measures, including data protection by design and by default;
- security measures;
- personal data breach notifications;
- data transfers outside the EU; or
- dispute resolution procedures.

Trade associations or bodies representing a sector can create codes to help their sector to comply with the GDPR efficiently and cost-effectively.

Source: Point 8 of the guidelines pg. 7.

Even though sectoral codes of conduct are voluntary, there are nevertheless procedures relating to Art. 40 and 41 of the GDPR in terms of the rules involved in the submission, approval and publication of codes at national and European level. A voluntary approach could potentially be effective, but this implies high levels of awareness among manufacturers about the risks and security vulnerabilities within products to spur industry to take proactive steps to address risks through self-regulation.

There have also been **developments in technological solutions** that could improve data protection and privacy, and enhance cybersecurity, such as the "security by design" concept, which has led to the development of methodologies and standards to improve product safety. Examples were provided in Section 4.2.3 (technical solutions).

5.1.5 Policy Option 2, 3 and 4 – A regulatory approach

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. Mandatory requirements would be introduced for manufacturers to ensure that their products were secure in relation to ensuring safeguards for data protection and privacy, and for protection from fraud.

The degree to which a regulatory approach might contribute towards the achievement of policy objectives relating to ensuring data protection and privacy and safeguards to ensure protect against fraud for internet-connected RE has been considered.

Before considering the sub policy-options, it is important to present the overall findings in relation to the relative advantages and disadvantages of a regulatory approach from the perspective of different stakeholders:

A concern was expressed by several stakeholders (industry associations, but also some national authorities) that a mandatory regulatory approach covering only internet-connected RE products subject to the RED would **risk leaving gaps in product coverage.** This could lead to an uneven playing field as the legislation would not cover the risks for data protection and privacy and protection from fraud for wired connections. Some security vulnerabilities are applicable to all internet-connected RE, irrespective as to whether these involve online penetration when a device is internet-connected, of offline physical penetration.

Some industry associations representing SMEs defended the benefits of a regulatory approach, stating that relying on industry self-regulation would be insufficiently effective and would effectively mean continuing with the status quo (Option 0). SMEs suggested that activating the DA would provide a legal mechanism to allocate clear responsibilities between hardware and software vendors for ensuring that basic minimum security requirements for internet-connected RE are integrated from the outset.

Many stakeholders were in favour of a horizontal piece of law dealing with cybersecurity, which could be made applicable to all industrial products (wireless and wired) rather than a RED-specific approach, which would only cover wireless. Some stakeholders argued that if (minimum) baseline cybersecurity requirements were integrated into the RED, there will be implications for industrial product legislation more widely in that over time, such legislation will also have to integrate security baseline requirements and cybersecurity considerations.

Other industry associations were in favour of adopting a more holistic and comprehensive approach to ensuring security of internet-connected RE products placed on the European market across all industrial product legislation rather than legislating through the RED's delegated acts. However, this was **only realistic in the medium term since whereas the delegated acts are already mentioned in the 2014 RED, possible legislation on cybersecurity might take 5-10 years to develop.**

Consumer associations and MSAs were generally of the view that activating the delegated acts for connected RE products would be an important starting point as regards their percentage market share. An estimated **70-80% of the total market is wireless,** according to estimates made by several stakeholders in interviews and also the targeted consultation findings.

Therefore, activating the two DAs under the RED would provide a positive step in the right direction to protect users. Enacting a regulatory approach through the DAs was therefore seen as a better and more effective approach than taking no regulatory action at all, and/ or waiting until such time as a consensus emerged on a horizontal law on cybersecurity.

Activating the DAs would make EO in the market responsible or accountable for putting safe products on the market. A regulatory approach would involve giving MSAs the necessary enforcement powers to remove products from the market through the issuing of product recalls. This would protect consumers and professional users of insecure internet-connected RE.

Stakeholders noted that a regulatory approach should favour activating both DAs at the same time, as there is a blurring between Article 3(3)(e) and 3(3)(f) in many areas, although sometimes the security issues – and potential technical solutions – differ.

Stakeholders noted that the main disadvantage of a regulatory approach would be the administrative costs for industry. However, these would be offset against the cost of breaches of internet-connected RE personal data have occurred, reputational damages or lack of consumer trust surpasses the cost of integrating security into IoT products. It is in fact more cost-effective to adopt a security-by-design approach, rather than to fix security issues retrospectively.

In terms of other disadvantages, an interviewee noted that there is sufficient regulatory protection to protect RE devices (e.g. Art 25 of the GDPR or the Cybersecurity Act) because they already provide the necessary tools to regulate the market.

Industry associations have adopted the rationale that technical solutions should be determined by manufacturers, instead of the legislator. There have been concerns regarding the administrative costs for manufacturers of internet-connected RE and wearable RE if they were made responsible for ensuring that products and devices were compliant. However, some stakeholders were more concerned about Art. 3(3)(i) the duration of software and firmware updates than they were about data protection and privacy (where they are already subject to requirements under the GDPR) as there would be costs incurred post-placement on the market. Although software updates are necessary, it is difficult for manufacturers to check ongoing compliance when they are not in direct control of the software, which is commonly developed by third-parties rather than the manufacturer.

Overall, a voluntary approach was seen as being less administratively costly by industry, but would still leave the regulatory gaps identified in Policy Option 0.

Policy Options 2, 3 and 4 are now examined, which all fall under a regulatory approach, and would involve either activating Article 3(3)(e), Article 3(3)(f), or both.

5.1.5.1 Policy Option 2 - Adoption of a delegated act pursuant Article 3(3)(e).

This option would involve activating Article 3(3)(e) within the RED, with mandatory requirements to ensure that internet-connected RE integrates safeguards to ensure that the personal data and privacy of users of connected RE and wearables are protected. The desk research found that:

- Mandatory minimum baseline security requirements to ensure adequate data protection and privacy have already been integrated into specialist internet-connected RE through the Medical Devices Regulation (Regulation (EU) 2017/745). The rationale for regulating medical devices first was that products equipped with radio devices such as pacemakers are high-risk were they to be hacked or accessed on an unauthorised basis. Indeed, there have been a number of hacking scandals and security vulnerabilities identified [152]globally.
- The literature review and some interview feedback suggested that the scale and magnitude of the problem of security vulnerabilities in internet-connected RE and wearable RE has got progressively worse in the past 5 years, particularly for consumer IoT devices.
- Since a small number of regulatory gaps were identified as regards data protection and privacy in the EU legislative framework, a consequence of inadequate protection is that users would remain at a risk of security breaches occurring, leading to a risk of personal data loss, privacy being compromised, and a risk of fraud occurring.

The interview feedback from stakeholders regarding the possible activation of a delegated act pursuant Article 3(3)(e) was mixed. There were divergent views as to whether a regulatory approach to ensuring device-level security in internet-connected RE and wearable RE could ensure data protection and privacy.

Some stakeholders were not in favour of additional regulation. They made a number of arguments in this regard:

- Several leading industry associations, such as those representing the digital sector, and national domestic appliances manufacturers, said that their members were against a further extension of

[152] See articles such as “A New Pacemaker Hack Puts Malware Directly on the Device” https://www.wired.com/story/pacemaker-hack-malware-black-hat/ and https://www.csoonline.com/article/3296633/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html

the RED's current essential requirements as:

  - The additional compliance costs of extending the essential requirements through the activation of the two delegated acts within scope;
  - The risk that those already compliant with the RED's essential requirements under Art. 2 would bear any additional costs of extending the essential requirements through Article 3(3)(e) and Article 3(3)(f). The main concern was that non-compliant manufacturers with the current essential requirements manage to get away with being non-compliant, due to challenges in market surveillance being able to remove such products on a timely basis, and that those disregarding their existing legal obligations would be unlikely to implement new obligations, whereas more responsible manufacturers would comply with any new requirements. It was argued that this would put them at an unfair competitive advantage, without more resources being devoted at national level to market surveillance and enforcement activities, where resources are already stretched in many countries;
  - However, other stakeholders countered this, as the best known manufacturers already invest heavily in product security as an inherent part of the brand's value;
  - Some stakeholders were also concerned about the risk of duplication in costs for manufacturers if their industry is taking part in developing certification schemes under the CSA as this has only recently come into effect. A further point was that some industry participants view the CSA as being *de facto* mandatory already if their particular product category or industry decides to adopt such as scheme. Even if it is formally non-mandatory, those procuring services will demand that industry is compliant.
  - Whilst in principle, any administrative compliance costs incurred under the RED would be mitigated if the manufacturer were already compliant with a cybersecurity certification scheme under the CSA, there was a perceived risk that technical standards for the RED will differ from such certification, requiring them to carry out compliance testing for moderately different security requirements more than once, leading to duplication of costs.
  - However, the Commission could undertake to ensure coherence between the different legal requirements and across technical solutions to check that wherever possible, duplication of costs, especially as regards costly testing costs, were avoided. Nonetheless, manufacturers were concerned as they stated that testing for product certification schemes will differ with testing against new harmonised technical standards. Therefore, the important issue of whether mutual recognition of technical solutions across different pieces of legislation (whether mandatory, such as the GDPR's Art. 25 or voluntary, like the CSA) will be needed.

- The CSA has not yet been fully piloted through the development of product certification schemes. Before further regulation is adopted, for instance through the activation of the two delegated acts within the RED, it was argued that the effectiveness of implementing a voluntary approach under the CSA should be evaluated. An argument against this however is the amount of time it will take before the CSA's effectiveness can be assessed.
- A further argument put forward was that current legislation should already be sufficient to protect consumers, especially GDPR (personal data protection and privacy). However, as noted earlier in the assessment of Policy Option 0 this was recognised as being contingent upon relevant Articles within the legislation being implemented and enforced more effectively, particularly Art. 25 (data protection by design and by default). Moreover, there is a further gap that if the manufacturer of internet-connected RE and wearable RE does not intend to collect any personal data, they are presently GDPR-exempt (a gap that could be addressed through the activation of the RED's DAs)

Conversely, other stakeholders (some industry associations, consumer associations, many national authorities and MSAs) were either strongly in favour, or generally in favour, of a regulatory approach.

Among the arguments put forward in this regard were that:

- The existing regulatory framework was seen as being insufficiently fit for purpose to address security vulnerabilities in internet-connected RE. Therefore, relying on existing legislation would not be fully effective, as:
    - As explained under Policy Option 0, whilst the GDPR provides a legal basis for issuing fines and for DPAs to pursue legal cases, non-compliant products cannot be removed from the market by MSAs. The RED does not presently provide a legal basis either as the delegated act foreseen in Article 3(3)(e), which has not yet been activated.
    - Risks for users cannot be addressed directly, but only indirectly (for instance, through fines issued under the GDPR to non-compliant data controllers and processors).
    - Current EU legislation does not provide any protection from fraud, nor a definition of what fraud means in the context of users of internet-connected RE devices and products.
- The regulatory authorities responsible for monitoring and enforcement of the implementation of EU data protection legislation (data protection authorities) differ from those responsible for industrial product legislation (market surveillance authorities). There is often an absence of sufficient coordination between such enforcement authorities, as the legislation for which they each respectively have responsibility for monitoring and enforcement differs.
- If there were to be a continued reliance upon existing EU legislation on data protection and privacy as a mechanism for changing manufacturers' mindset, and embedding security by design and default principles into product design, engineering and manufacturing, this could be a missed opportunity according to some stakeholders to address the identified security vulnerabilities.
- Security vulnerabilities in internet-connected RE and wearable RE could better be addressed through technical solutions, such as baseline security requirements developed by ENISA, NIST and others. This was seen by some manufacturing associations and cybersecurity associations as being more effective than relying on the GDPR.
- Doubts were expressed among some stakeholders as to whether national DPAs are sufficiently familiar with industrial products and with how EU industrial product legislation is implemented, monitored and enforced. Expertise to check the compliance of internet-connected RE and wearable RE for minimum baseline security requirements lies with testing bodies and MSAs rather than with DPAs. This strengthens the argument that relying on proactive enforcement of the GDPR as implemented by industry may not be the most effective regulatory approach.
- Rather, the principles in the GDPR as regards data protection and privacy arguably need to be translated into more technical rules and customised so that they are applicable to industrial products (in this case, connected RE products and wearable RE), so long as it is made clear how the GDPR requirements for data protection by design and default differ from the requirements that would be introduced through the activation of Art. 3(3)(e). One key difference is that if new essential requirements relating to data protection and privacy were activated, then technical solutions would need to be developed in the form of harmonised technical standards which is not the case under the GDPR, where no such standards exist.

Overall, Option 3.1 was assessed as being viable. The legal analysis presented in Section 3.3.1 found that a regulatory approach under which mandatory requirements relating to ensuring data protection and privacy could help to address a number of regulatory gaps. However, it should equally be acknowledged that whilst legislation would strengthen regulatory certainty and effectiveness in the area of data protection and privacy, relevant stakeholders (especially industry associations) have conflicting views. Nevertheless, there was evidence of reasonable consensus of the need for a regulatory approach among some stakeholders (cybersecurity associations, MSAs, many but not all national authorities).

5.1.5.2 Policy Option 3 - Adoption of a delegated act pursuant Article 3(3)(f).

This option would involve activating Article 3(3)(f) in the RED, and introducing mandatory regulation for EO to ensure that connected RE products, especially consumer IoT products and wearables integrating RE have a minimum level of cybersecurity in respect of protection from fraud. The findings in relation to the analysis of stakeholder feedback on protection from fraud are now presented.

The research identified a number of **different examples of how fraud might be perpetrated due to insecure internet-connected RE**, including: the risk of geolocational data not being protected from third parties; software and firmware updates not taking place beyond a certain period post market placement; a lack of a verification and authentication process before internet-connected RE is paired with Bluetooth devices; insufficiently secure storage of users' personal data; a lack of password-protected access; and poor authentication requirements to identify the user. Collectively, these weaknesses mean that internet-connected RE and wearable RE security can be breached at the device level. [153]

There is an issue as to **how far the RED can realistically combat fraud without a more holistic approach** extending beyond the RED. The literature review found that the main ways in which internet-related fraud is perpetuated is via an email, such as via malware or via a browser. In other words, the risks relate to software on the device and to incoming communications to the device rather than relating to elements of the device itself before the RE is placed on the market.

There is limited existing EU legislation on fraud and currently **no laws that directly addresses the need to strengthen security to protect consumers from fraud in respect of internet-connected RE**. The Non-Cash Payments Directive (EU) 2019/713 is concerned with tackling fraud in connection with alternative means of payment, such as cryptocurrencies, but does not address the security of RE.

The **legal text of the RED does not contain any definition of 'protection from fraud'** in Article 3(3)(f). However, examples of different types of fraud that can be perpetuated through fraudulent access to internet-connected RE and wearable RE have been identified.

However, not all stakeholders thought that the absence of a definition of fraud was a problem. Indeed, some stakeholders pointed out that **security threats evolve and change constantly,** and therefore, as soon as a definition and illustrations as to what constitutes fraud means, the nature of the threat is likely to change. For example, fraud may involve hacking, and financial theft is often the main motivation. However, it can also involve identity theft, which can be monetary, but may also be driven by other motivations. Further to this, demonstrating the links between Article 3(3)(e) and Article 3(3)(f), data is a type of currency, so anything that is linked to the misuse of data could also be considered as fraudulent. The latter issue would not have been considered fraudulent even 5 years ago, but the GDPR has had an impact in this regard.

Activating Article 3(3)(f) could have a positive impact on the market, according to some stakeholders who highlighted the importance of harmonising standards and adopting a broad, precise and technically-neutral definition of fraud, so manufacturers would have greater regulatory certainty when developing their products. If Article 3(3)(f) is not defined in a clear and precise way, its implementation and enforcement at industry-level will be limited.

Some stakeholders argued that fraud could be more effectively tackled through national criminal legislation. However, **in an internal market context, this would not support the free movement of products,** as there would be a reliance on heterogenous national legislation to combat the problem retrospectively (i.e. once a fraud has been perpetuated) rather than tackling the problem before products have been put on the European market by tackling security vulnerabilities at the design stage. This would minimise the risk of fraud once internet-connected RE and wearable RE has been

[153] It should be noted that the RED is only concerned with devices, and not with network-related risks relating to data protection and privacy, which are covered through the e-PD.

placed on the market and the products, devices and equipment are actually being used.

Many stakeholders pointed to the **close inter-relationship between data protection and privacy and protection from fraud.** It would arguably be difficult to legislate for one of these elements through the RED without regulating both. For example, loss of personal data, unauthorised access to personal data, privacy breaches and instances of fraud may materialise if there is an online penetration of a RE device/ product by an unauthorised third party. Moreover, when looking at technical solutions, it is very difficult to distinguish solutions that would only ensure safeguards for data protection and privacy without addressing the risk of fraud and vice versa.

The main perceived drawback of going ahead with activating Art. 3(3)(f) is that whereas there are many technical standards focusing on cybersecurity more broadly, security standards focusing on fraud tend to be concentrated on **protecting novel forms of online and near-field communication contactless payments**. Fraud prevention more broadly is not an area that has previously been regulated at EU level. However, this is because relevant technical security standards in the field of cybersecurity will prevent device penetration which in turn will prevent fraud alongside the theft of personal data (reflecting the interrelationship between Art. 3(3)(e) and Art. 3(3)(f). Reference should be made here to Section 4.2.3, which outlines the findings from the mapping of existing technical solutions to combat fraud.

5.1.5.3 Policy Option 4 - Adoption of both delegated acts pursuant both Articles 3(3)(e) and (f).

Policy Option 4 would involve the adoption of both delegated acts.

Feedback from interviews suggests that a regulatory approach would only be coherent if Article 3(3)(e) and Article 3(3)(f) were to be activated in parallel. Moreover, many stakeholders pointed to the need for a holistic approach to security which recognises the inter-relationship between not only Article 3(3)(e) and Article 3(3)(f), but also Article 3(3)(d), the prevention of Botnet attacks. There have been many examples of large numbers of insecure internet-connected RE and wearable RE 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. The inter-linkage between consumer IoT device-level risks and network risks is important and should not be under-estimated. However, it will be the subject of a separate study expected to be undertaken in 2020. Many interviewees specialising in cybersecurity and some industry stakeholders were worried about botnet attacks and supported regulatory intervention.

Many stakeholders noted that the interaction between the two delegated acts Article 3(3)(e) and Article 3(3)(f) is close, and that this should be factored in when doing any detailed technical planning, were the two DAs to be activated. For example, a stakeholder mentioned that 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, which makes the distinction and delineation between the two DAs blurry. It would be contradictory to differentiate between safety and security – products will not be safe if they are insecure.

Among many manufacturers of internet-connected RE and industry associations, the main concern as regards activating the two DAs is that administrative costs would be incurred by industry, especially due to testing.

However, the costs of strengthening the security of internet-connected RE should be offset against the high costs of data breaches leading to losses of personal data, the reputational damage done to the producers and/ or third party service providers concerned and the economic impacts of reduced consumer trust (see section 5.2.1 which considers the costs of non-action under economic impacts). Data has a value and protecting such data by strengthening the security of internet-connected RE and wearable RE implies costs, but these are lower than the alternative of not acting to prevent data breaches.

A security-by-design and default approach could be cost-effective in addressing security vulnerabilities. There is already a data protection by design and default approach under the GDPR. Evidence that such an approach could be more efficient than alternatives was cited by some interviewees. Software was cited as an example, as it was considered to be much less costly to design a secure product before products are placed on the market, rather than to discover multiple security vulnerabilities retrospectively and to then have to make frequent software updates and to issue patches as and when new vulnerabilities are identified. However, in practice, this may be easier said than done as bugs are often discovered in software post market placement (outside the scope of this study but covered in the other study on Art. 3(3)(i)).

The main advantage of PO4 from a consumer and end-user perspective is that internet-connected RE and wearable RE would be strengthened through improved security. Many stakeholders pointed out that a product cannot be fully safe unless it has been adequately secured.

Activating the DAs would make manufacturers directly responsible (and accountable across the value chain when working with service providers and other third parties) for putting safe products on the market. A regulatory approach would involve giving MSAs the necessary enforcement powers to perform product recalls to protect consumers.

Feedback from the interviews found that Articles 3(3)(d) and 3(3)f) are better articulated in the RED than anywhere else, because they cover digital software and physical products, whereas Article 3(3)e is already covered to some extent in the GDPR, although the fact that there is no scope for MSAs to recall internet-connected RE and wearable RE. Separating software from physical products would leave a gap on the market – there is a need for a legal basis to deal with both aspects at the same time.

If the two DAs were to be activated, then industry stakeholders (industry associations and manufacturers) stated that these would have to provide clear, but broad definitions of what ensuring data protection and privacy and safeguards protection from fraud actually means.

Moreover, it was stressed that the definition should not be overly descriptive or prescriptive and should remain technologically-neutral to allow for the specific basic security functionality of particular IoT products to be developed through harmonised technical standards. These will need to be adapted and updated progressively over time so as to strengthen cybersecurity resilience in the face of evolving threats and vulnerabilities.

Useful recent developments in respect of technical solutions could be relevant to the possible activation of both DAs. A case in point is the development of ETSI TS 103 645.

Several stakeholders welcomed the development of the ETSI standard, although it was stressed that this only provides an umbrella framework and a starting point for the possible future development of harmonised technical standards.

If a regulatory approach were to be adopted, involving both DAs being activated, then several stakeholders raised the issue as to the need for careful implementation in terms of how new essential requirements relating to data protection and privacy and safeguards to ensure protection from fraud might be rolled out. Here, the issue is whether it would be realistic to make all categories of connected RE across all products subject to cybersecurity requirements immediately.

The interview feedback suggests that there would be greater costs for some products than others, for example, the need to integrate encryption technologies in some categories of internet-connected RE and wearable RE that were not previously required to do so. Some sectors may therefore need more time to adapt, and also, technical standards have not yet been developed at the product level, therefore there is a question mark as to how regulation would work in practice.

If one or both delegated acts were to be activated, there should be a “big bang” approach, whereby all internet-connected RE products would have to comply with the essential requirements relating to

i) data protection and privacy and ii) protection from fraud from the first day or whether an incremental approach should be adopted whereby baseline security requirements were introduced sequentially on a product-by-product basis.

- In this regard, it is worth recalling the technical complexity of implementing consumer IoT technical standards, given that to date, there is only a single European umbrella standard, ETSI TS 103 645, and harmonised product-specific standards have not yet been developed at European level pertaining to consumer IoT security.
- Moreover, the CSA has adopted such an incremental approach, relying on voluntary certification schemes, requiring cooperation between ENISA, standardisation bodies and industry. Likewise, the Ecodesign Directive has adopted a hybrid regulatory model which combines mandatory eco-design requirements with a voluntary, sector-by-sector approach to determining the technical requirements for eco-design at the product level. An issue for debate during the remainder of the study is whether if a regulatory approach is identified as the preferred option, how should this be implemented.
- A further issue is the **need for a value chain wide approach** to improve the security of internet-connected RE and wearable RE, irrespective as to which technical solutions are implemented. A position paper by the European Digital SME Alliance [154] makes clear that *"In the digital age, the security of complex manufacturing processes and industrial supply chains will not only depend on high cybersecurity standards in tier-1 suppliers or Original Equipment Manufacturers (OEMs), but also the level of cybersecurity assurance in companies along the supply-chain pyramid (i.e. tier-2 or tier-3 suppliers)".*
- The paper also notes the interconnectedness between standards and certification schemes. Furthermore, the paper notes that "Cybersecurity certifications could be disruptive as they will allow consumers with limited technical literacy to make an informed choice about the security of a certain product, service or process". This is an important point in that many stakeholders in the interview programme mentioned that **although minimum baseline security standards could make a positive difference, ultimately, ensuring that internet-connected RE products are more secure requires a partnership between the ESOs, industry and users.**

5.1.6 Policy Option 5 – a horizontal piece of legislation on cybersecurity

A potential fifth policy option could be to consider the introduction of a horizontal piece of legislation on cybersecurity. This option was not identified explicitly in the study's ToR but has been suggested by a number of stakeholders in the interview programme and in response to the targeted consultations.

A number of stakeholders – especially industry associations and individual manufacturers - raised the issue that they did not perceive a differentiated regulatory approach between wireless products subject to the RED and wired products to be fair, as it could undermine the concept of a level regulatory playing field.

However, they also recognised that there may be a need to take regulatory action in future to ensure that products are cybersecure by design and default as a pre-requisite to ensure that they also meet data protection by design and by default rules under the GDPR. Furthermore, although existing legislation focuses on data protection, for example through data protection by design and default (Art. 25 GDPR), the majority of literature and good practice guidelines focus more on security by design and default. Therefore, several stakeholders, including some of the major European industry associations, suggested that it would be preferable to introduce a single mandatory piece of legislation on ensuring minimum baseline secure requirements to ensure that all connected RE products are cybersecure and

[154] The EU Cybersecurity Act and the role of standards for SMEs - Position paper, European Digital SME Alliance, Brussels, 14 January 2020

thereby also ensure through technical solutions, such as encryption and authentication, higher levels of data protection and privacy and protection from fraud.

It was however pointed out for example in discussions in June 2019 at the Radio Equipment Expert Group (RE EG) that realistically, given legislative timeframes, such an option could only be considered over the medium term as it might take up to 5 years for consultations to take place, then a regulatory proposal to be developed, and subsequently for scrutiny through the co-legislative procedure. An overview of the advantages and disadvantages of Option 5 is provided below:

Table 5.2: Overview of the advantages and disadvantages of Option 5

Advantages	Disadvantages
• Would cover both wireless and wired products • Level regulatory playing field (e.g. depending on how RE device is connected (direct/ indirect, wireless/ wired)	• Timeframe to adoption, coming into effect, implementation and enforcement of the new legislation. • Urgency – many stakeholders expressed view that problem needs tackling more urgently than a new Cybersecurity law covering all industries products would allow. • Missed opportunity to take action now as the delegated acts have already been agreed under the new legislation.

5.2 Analysis of Impacts

In this section, an analysis is provided as to the different types of impacts – economic, social and environmental – that could materialise under the different policy options. It should be noted that the assessment is primarily qualitative as it was not possible to quantify the impacts. The reasons why there were difficulties in quantification are explained later in this section. However, a few of the economics benefits have been quantified in Section 5.3.9 (benefits of activating the delegated acts).

Regarding the analytical framework for assessing impacts, the European Commission's inception impact assessment [155] contained examples of the types of impacts that might be expected to occur if the two delegated acts were to be activated. In the following table, examples of these mainly qualitative impact indicators are provided.

Table 5.3: Inception impact assessment report

Economic impacts	**Micro and meso level impacts on manufacturers of RE devices and wearable RE.** • Increased capacity of producers located or selling into the EU to make their products secure prior to them being placed on the European market. • Increased resilience against fraud and avoidance of economic loss to consumers and industry of fraud. • Strengthened competitiveness of EU industry by focusing on cybersecurity as a competitive strength. **Macro-economic impacts** • Improved functioning and harmonisation of the Internal Market. • Corresponding improvements in terms of fair competition – level playing field avoiding the creation of national legislation on IoT.

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

	• Stimulation of the development of the Digital Single Market and improvements in the data protection and privacy field.
Social impacts	• Increased security and safety for EU citizens (specifically some vulnerable users, e.g. children) in the digital society and economy. • Increased protection of personal data and privacy • Increased consumer trust in the Digital Single Market and the digitization of traditional goods; • Resilience against illicit practices (e.g. increased cybersecurity of the concerned products, prevention of frauds);
Impacts on the environment	• The IIA consultation document states that “No specific or major impact on the environment is expected”.

Source: CSES analysis of published inception impact assessment.

The study team has assessed:

- The extent to which the analysis of the findings from the inception IA carried out by the Commission in Jan- March 2019 identified the same types of impacts as the stakeholder consultations undertaken as part of this IA;
- Views on the likely scale and magnitude of the impacts, both positive and negative, depending on which policy option is adopted;
- The impacts by stakeholder type; and
- The issue as to whether there may be any unintended consequences and impacts.

The feedback obtained through the interview programme by type of impact and stakeholder is now examined:

5.2.1 Economic impacts

Feedback on the economic impacts was sought, taking account of the different policy options defined.

Some stakeholders, such as consumer associations and cybersecurity industry organisations, argued that there could potentially be economic benefits of a regulatory approach, and in activating the DAs. Examples were:

- **Increased sales volumes of internet-connected RE and wearable RE due to strengthened trust among users.** Reference should be made to Section 5.3.9, which seeks to quantify the potential benefits of enhanced trust. Improvements in ensuring that internet-connected RE and wearable RE is secure, and that personal data protection and privacy are safeguarded, should promote increased sales, . These are already forecast to grow significantly, but could grow even faster (by 5-10% extra) if products were made more secure[156]
- **Mixed evidence as to whether mandatory minimum security baseline requirements for internet-connected RE and wearable RE would lead to reduced prices. The impact on prices may be neutral as there would be some additional costs, but these would be offset.** There may be minor cost increases, for instance, due to manufacturers having to invest in strengthening the security of such RE in the design, engineering and manufacturing stages, with direct costs incurred if specific technical solutions are required (e.g. authentication and encryption). However, these additional costs could be offset for instance by faster sales growth of internet-connected RE and

[156] See data on internet-connected RE and wearable RE forecasts in Annex 5, which outline key demand-side trends. These are summarised in Section 3.1.1.

wearable RE (especially of consumer IoT products and devices that fall under the RED) due to enhanced consumer trust. There would potentially then be benefits through economies of scale, and therefore a downward impact on prices.

- **Strengthened competitiveness of EU industry,** for instance, by:
  - **Reducing substantive compliance costs for producers.** There would therefore be economic benefits from a cost savings perspective in designing-in security requirements from the outset in accordance with a security by design approach. These requirements could be set either on a mandatory basis through mandatory harmonised technical standards or voluntary certification schemes (f e.g. product-specific consumer IoT certification schemes through the CSA). Addressing security concerns post-placement on the market would be costlier for manufacturers than integrating security by design from the outset.
  - **Reducing reputational risks for economic operators** – reputation management is an important part of intangible value for large manufacturers, for after-care service provision and for service providers. If there were greater certainty pertaining to the integration of minimum baseline security requirements into the essential requirements (focusing on data protection and privacy/ protection from fraud), this would ensure that manufacturers and other economic operators in the value chain took steps to embrace a security by design and default. This would in turn reduce reputational risks and the potential risks post-market placement of costly data breaches.
- **Benefits from lower incidence of fraud, thereby avoiding direct economic losses for consumers and reduced reputational and insurance liabilities for industry.** Whilst there are specialist insurance providers that offer insurance against costly data breaches, the costs of such insurance would be reduced if appropriate minimum baseline security features were integrated into internet-connected RE and wearable RE from the outset.
- **Improved functioning of the Internal Market by ensuring that a level playing field is maintained without the emergence of national divergent legislation.** Without the activation of the two DAs, there is a risk that some Member States legislate at national level to strengthen the security of internet-connected RE and wearable RE prior to products being placed on the market. This would undermine the internal market in the circulation of such products.
- **Avoiding unnecessary barriers to the Digital Single Market (DSM). Greater public trust in, and recognition of the benefits of the DSM.** Consumers have the right to expect products to integrate at least basic minimum security requirements in internet-connected RE.
  - **Facilitating exports to new EU markets.** European manufacturers complying with essential requirements relating to cybersecurity could use compliance with corresponding harmonised technical standards in their marketing, thereby helping to develop new export markets;
  - Reduced risk of data controllers and data processors being issued with fines for GDPR breaches in relation to non-compliance with Art. 25 (security by design and default).
- Overall, strengthened security of internet-connected RE and wearable RE could have positive sectoral level and macro-economic benefits resulting from a bigger overall market for such RE.

The main findings as regards the **economic costs of non-action** were that:

- According to many European and national consumer associations, as well as by specialists working in the cybersecurity industry, there could be adverse economic (and social) impacts if consumer trust in internet-connected RE and wearable RE is undermined due to the increasing prevalance of scandals.
- It was acknowledged by some manufacturers that not all internet-connected RE and wearable RE are adequately secure, which risks undermining the reputation of industry for some product

categories. Moreover, the literature review identified the need for such RE to be designed and manufactured in a more secure manner so as to realise the full benefits of the Digital Single Market (DSM). *"The potential benefits will only be achieved if services and products can be designed with trust, privacy and security built in so that consumers feel they are fair and safe to use. This will be essential to building a trusted IoT environment for consumers"*[157].

More limited stakeholder feedback was obtained in respect of the potential benefits of the other policy options. For instance, the suggested benefits of a non-regulatory approach were:

- Reduced administrative costs for manufacturers, compared with a mandatory approach, as there would be less testing required.
- Greater flexibility to make use of existing industry bodies that play a coordination role in working across particular industry sectors and sub-sectors in developing industry-led standards, thereby potentially avoiding duplication with the work of the three European Standardization Organisations (ESOs).
- The scope for enhanced trust among users in purchasing internet-connected RE and wearable RE if good practices were disseminated and adopted by manufacturers voluntarily.
- Through the use of certification schemes developed under the CSA, an opportunity for industry to export more products to third countries, since product security is often used by European and large global manufacturers as an asset in their branding.

  However, the potential benefits of a non-regulatory approach or of the status quo option will only be realised if there is widespread buy-in by industry to good practices as regards security by design and default.

5.2.2 Social impacts

Regarding the social impacts, two aspects were explored, firstly the costs associated with non-action, since there could be adverse impacts as regards the risk of consumer detriment. Secondly, if EU level regulatory action were to be taken, then a number of potential benefits could emerge. The main findings were that:

- Insecure devices could be hazardous to ensuring product safety for consumers, as the RED's core objectives are arguably being undermined by the absence of essential requirements referring to product security. Several stakeholders pointed to the fact that an insecure product placed on the market cannot be deemed safe. This is insufficiently explicit in the current legislation.
- The continuing presence of insecure products on the market could have adverse effects on consumers, exposing them to threats such as data theft, financial fraud (including ransomware attacks), and identity fraud .
- Some literature points to vulnerable consumers being especially at risk of fraud, including children and the elderly, who are generally less aware about security vulnerabilities and threats in using internet-connected RE and wearable RE, or how to protect themselves given that these evolve rapidly. Whilst the possible introduction of minimum baseline security requirements could not guarantee protection, integrating a security by design and default approach to design, engineering and manufacturing, and implementing specific technical solutions would mitigate many risks, and thereby have social benefits for consumers.
- The activation of one or both delegated acts would have a number of social benefits:
  - **Greater security protection when using internet-connected RE and wearable RE , especially consumer IoT devices.** Many consumers generally, but especially vulnerable consumers such

[157] ANEC, BEUC, Consumers International, and ICRT. (2017). Securing consumer trust in the internet of things: Principles and Recommendations. https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf.

as children and elderly people, have low levels of cybersecurity awareness, knowledge and understanding. They would benefit from manufacturers being required to integrate baseline security requirements into the design and manufacturing stages, which is already the case as regards data protection and privacy by design and default through the GDPR, but it could be made clearer that this is applicable to all manufacturers and EO in the value chain. .

  - **Avoidance of unnecessary risk of consumers' personal data being compromised, and of fraud being committed.** Whilst feedback from all types of stakeholders interviewed and responding to the OPC and targeted consultations recognised that it would be impossible to eliminate the risks of the unauthorised penetration of internet-connected RE and wearable RE, users would benefit if the most basic security requirements were mandatory. This would minimise the risk of data breaches and the misuse of personal data. Industry associations and manufacturers also stressed the importance of users needing to take responsibility in parallel to improve their cybersecurity awareness when using internet-connected RE and wearable RE, especially for consumer IoT devices.

- **Wider societal benefits.**
  - The longstanding concept of a **rights-based approach to protecting users' personal data and to ensuring their privacy** was initially set out in Directive 95/46, [158] applicable since 1995. Since the GDPR came into effect in May 2018, this concept has become better known. A positive impact of the GDPR is that consumers are more aware about their right to minimum security to ensure data protection and privacy and protection from fraud. However, notwithstanding, regulatory gaps identified earlier (see the review of Policy Option 0) would need to be closed before the full societal benefits for citizens could be realised.

In terms of the social impacts of the other Policy Options, under Option 1 (a voluntary approach), the adoption of voluntary industry codes of conduct and certification schemes by product group under the CSA could also contribute towards the above-mentioned benefits. For instance, users of internet-connected RE and wearable RE (especially consumers) would also benefit from greater protection in using internet-connected RE if products are developed in accordance with new certification schemes under the CSA, and could also make more informed choices when using IoT and / or ICT security labels.

However, a key difference between a mandatory and a non-mandatory approach is that **consumers' rights would be less well protected**. Under a voluntary approach, whilst consumers would continue to be partially protected under existing legislation. For instance, consumers are protected under the GDPR (so long as it is clear that the manufacturer has been designated as a data controller and intends to collect and process data, and they are responsible for monitoring other EO within the value chain designated as data processors. Those product categories where certification schemes exists under the CSA would also be protected. . However, without mandatory legislation there would be less certainty as to whether safeguards to ensure data protection and privacy and protection from fraud could be ensured across all connected RE product groups. Therefore, the anticipated social impacts would only materialise partly without a regulatory approach.

5.2.3 Environmental impacts

Compared with economic and social benefits, there was less stakeholder feedback on the potential environmental impacts. However, a working hypothesis has been developed by the study team based on a combination of desk research and some interview feedback.

Firstly, from an EU policy perspective, if the RED's essential requirements were to be extended to include cybersecurity (data protection and privacy and protection from fraud) through the development of harmonised standards integrating security by design and default principles, this could

[158] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

in principle contribute to strengthening the circular economy and sustainability, which have a renewed importance in the context of the Green Deal.

In particular, some large manufacturers commented that there remain some **low-quality and very cheap internet-connected RE products on the European market that are non-compliant.** In their view, these should be removed from the market by MSAs either because they are unsafe (and covered by the RED's existing essential requirements) or because they are insecure (and could be covered through the activation of Article 3(3)(e) and 3(3)(f).

Removing such products from the market could translate into **European consumers purchasing better-quality internet-connected RE and wearable RE as insecure products could not legally be placed in the market.** Encouraging EU citizens as consumers to shift up the value chain and purchase better quality internet-connected RE, such as electrical equipment and household appliances could help to reduce purchases of cheap quality equipment with a shorter product lifecycle. This in turn should help by:

- **Contributing to the circular economy and sustainability** by lengthening the average lifespan of the use of such internet-connected RE, and reducing unnecessary use of raw materials;
- **Reducing the tonnage of electronic and electrical waste generated across the EU-28** each year (regulated under the WEEE Directive 2012/19/EU). The amount of electronic waste could therefore potentially be reduced, or at least its growth could be partly mitigated by designing and manufacturing more enduring products;

In terms of how extensive this contribution would be, activating the two delegated acts would cover an estimated 70-80% of all internet-connected radio equipment (wireless only, and therefore falling under the RED's scope).

Environmental benefits were however found to be contingent on more effective market surveillance and enforcement. A number of stakeholders noted that market surveillance by MSAs needs to be more proactive, such as greater investment in product testing and where non-compliant products are found, and their prompter removal from the market. This would be a pre-condition for the anticipated environmental benefits mentioned above to occur.

Some industry associations and manufacturers pointed to a general problem that non-compliant products with the RED's essential requirements have already been placed on the European Single Market, but often without being removed. Since these tend to be very cheap products of low quality, there was a concern that even if the DAs were to be activated, such products might remain on the market. This would prevent environmental benefits from materialising.

5.2.4 Unintended consequences and impacts.

In accordance with the Better Regulation guidelines, it is important to reflect upon any unintended consequences and / or unintentional impacts that could materialise under the different policy options considered.

Under **Policy Option 0, relying on existing legislation**, an unintended consequence could be that manufacturers don't take their obligations under Art. 24 and Art. 25 in particular seriously enough. A further unintended consequence could be that as some MS authorities asked the Commission to consider activating the delegated acts, if the Commission relies on existing legislation, MSAs could not remove internet-connected RE products and devices from the market that lack security functionality or which have been proven to compromise data protection and privacy of users (including products targeted at children). An unintentional effect is that national authorities may go ahead and legislate at national level instead to protect consumers, undermining the Single Market.

As regards **Policy Option 1 (a voluntary approach),** an unintended impact could be that manufacturers may be slower than under a regulatory approach to embrace security by design and default approaches to ensuring minimum baseline security. This could leave users unnecessarily at risk for longer, given the current proliferation of problems linked to hacking attempts and device penetration leading to data loss, and the widespread prevalence of fraud attempts via the internet. It should be stressed that these problems are not unique to wireless internet-connected RE products and devices, as they also affect wired internet-connected products. A voluntary approach may not lend the issue the necessary urgency that it needs.

Turning to Policy Options 2, 3 and 4 (a regulatory approach), there could also be unintended consequences and impacts of going ahead with the delegated acts. For example, there could be a risk that Art. 3(3)(e) could be perceived by some stakeholders as risking duplication with existing legislative requirements in the GDPR (data protection by design and default). Were the DAs to be activated, it would therefore be necessary to mitigate this risk by clearly explain in the drafting of the detailed text of the delegated act how the Commission will ensure coherence and consistency between the essential requirements in the RED and the legal obligations in the GDPR relating to data protection and privacy and under the e-PD / e-PR in relation to the privacy of e-communications data transmissions and processing.

5.2.5 Overall findings - impacts

In order to compare the different policy options, an impacts matrix has been developed, which considers across the policy options the extent to which there are likely to be positive, negative or neutral impacts. It should be stressed that sometimes the picture is more nuanced, however, as was explained in the analysis of the detailed stakeholder feedback provided in Section 5.1.

The table below brings together the analysis and considers the potential effectiveness of each option and the degree of impacts by type (e.g. economic, social, environmental).

Options	Effectiveness	Economic impacts	Social impacts	Environmental impacts
Option 0 - Baseline scenario based on existing EU legislation.	+/-	+	-	*
Option 1.1 - Industry self-regulation.	+/-	++	+	*
Option 1.2 - Regulatory approach, supported by accompanying measures, e.g. voluntary measures to help manufacturers achieve compliance (codes of conduct, awareness-raising)	++	++	+	*
Option 2 - Adoption of a delegated act pursuant Article 3(3)(e).	++	++	++	+
Option 3 - Adoption of a delegated act pursuant Article 3(3)(f).	++	++	++	+
Option 4 - Adoption of a delegated act pursuant both Articles 3(3) (e) and (f).	+++	+++	+++	++

Key:

- *Negative impacts – degree of magnitude differentiated between -, --, and ---*
- *Positive impacts – degree of magnitude differentiated between +, ++, +++*
- *Neutral impacts – **

The above table summarises the (preliminary) findings from the assessment of the impacts of the different policy options. The justification for the categorisation reflects the key findings from the assessment of policy options.

Relying on existing EU legislation would be somewhat effective, as the GDPR in concert with the e-PD would at least address some aspects of data protection and privacy, albeit with regulatory gaps (inability for MSAs to remove products from the market, although data protection authorities may issue fines for the passive transmission of data without permission). However, positive economic impacts that could be generated under a regulatory approach would not materialise, such as enhanced consumer trust and increased willingness to pay for products that integrate security functionality.

Moreover, there would be disbenefits of relying on existing EU legislation alone, such as negative economic and societal impacts if the risks of data breaches and personal data misuse are left unaddressed. Data scandals, breaches of personal data, reputational damage and/or a lack of consumer trust in IoT products have been recurring issues. Moreover, even if consumers have some level of awareness about cybersecurity, they are generally not aware about the evolving nature of such risks in relation to protecting their internet-connected RE devices (often consumer IoT).

A voluntary approach could potentially be effective, but only under the caveat of strong industry engagement, and a willingness to take active steps to strengthen consumer IoT cybersecurity. If this is not forthcoming, then there is a risk that in practice, market behaviours do not change and many connected RE products would remain unsecured. Indeed, several cybersecurity specialists suggested that the situation has worsened in the past 12-24 months, rather than improved. Again, this would mean that the economic benefits that could be possible under a regulatory approach would not materialise.

In such a situation, an adverse impact for consumers purchasing connected RE products is that they would remain generally unprotected, with variations as to whether particular products embed basic minimum baseline security functionality in design and manufacturing.

Whilst consumers are already protected under the GDPR as regards data protection and privacy, there are no requirements for manufacturers as regards ensuring security safeguards against fraud, thereby there is a risk of adverse social and economic impacts in terms of direct financial losses in the case of fraud and consumer detriment (upset and psychological harm from being the victim of theft). Under a regulatory approach, there would be societal benefits, as the risk of fraud would be reduced and consumer detriment would not occur.

The most positive impacts would arise if Option 4 were to be adopted, as the two delegated acts are inter-related, symbiotic and complimentary with one another. Therefore, maximising economic, social and environmental benefits implies activating the delegated acts as these would only occur under the regulatory scenario.

5.3 Cost-benefit analysis ("CBA") of the Policy Options

This section sets out the findings from the CBA.

5.3.1 Introduction to the CBA and methodology

The purpose of the **Cost-benefit Analysis** ("CBA") is to ascertain the costs and benefits of the different policy options. Qualitative stakeholder feedback on the drivers, costs and benefits, alongside any quantitative cost-benefit data estimates were collected through an **interview programme** with manufacturers, industry associations, testing and certification bodies, national administrations, and MSAs. The targeted **online survey** also informed the CBA, although costs data was only obtained from manufacturers and other EO.

The methodology required both qualitative and quantitative assessment. A supporting Excel sheet was developed, structured in a way that considered the methodological guidance in the **Better Regulation guidelines** pertaining to **CBA**. However, as there were methodological and data collection challenges in gathering quantitative data (for reasons explained below), it was not possible to use the full **Standard Cost Model (SCM)** approach.

Feedback was gathered through the stakeholder consultations on different types of **drivers of costs and benefits** for manufacturers of electrical equipment and household appliances containing internet-connected RE, and other EO in the value chain. However, major challenges were encountered in obtaining quantified data to inform the CBA. The analysis therefore relies on a combination of limited quantitative estimates of costs, but mostly on qualitative assessment.

5.3.2 Challenges in undertaking the CBA

There were a number of different challenges in obtaining quantitative data estimates on costs to inform the CBA.

Firstly, economic operators found it **difficult to estimate compliance costs.** Manufacturers stated that it was difficult to provide detailed costs estimates as the text of the delegated acts (DAs) has not yet been drafted. Moreover, they commented that it is not yet clear if the two DAs in scope were to be made mandatory, future harmonised technical standards would be adopted with common minimum requirements across different categories of internet-connected RE and wearable RE (on the basis that there are similarities in the risks), or whether these would be more product-specific.

For instance, ETSI standard TS 103 645 on consumer IoT security provides an umbrella framework for strengthening the security of consumer IoT devices. Although the study scope extends beyond consumer IoT, an important share of products within study scope that are problematic from a security point of view fall within this category of internet-connected RE. Whilst the above-mentioned ETSI standard embodies 13 good practice principles, it does not contain any product-specific requirements. The costs associated with implementing generic requirements that embed security by design and default principles would be lower than the comparable costs of implementing product-specific technical requirements. This meant that economic operators viewed there as being some uncertainties that make it difficult to estimate costs at this stage.

Further issues that made it difficult to estimate costs as regards the outstanding uncertainties as to how the two DA might be implemented are that:

1. The proposed text for the activation of the two delegated acts in scope is not yet available. Therefore, there was uncertainty among industry and manufacturers as to what minimum security baseline requirements might involve (although requirements developed by ENISA and NIST in this regard provide some examples).
2. It was unclear from a stakeholder perspective how far future harmonised technical standards are likely to be based on existing technical standards, such as international standards and industry standards. Costs would be difficult to estimate for manufacturers until examples of harmonised technical standards relating to the RED Art. 3(3)(e) are available.
3. It was seen as difficult to quantify the costs of either Art. 3(3)(e) or Art. 3(3)(f) as most technical standards focus on strengthening cybersecurity in general, by preventing unauthorised penetration of internet-connected RE. They do not specifically deal with data protection and privacy, and / or protection from fraud.
4. It is not yet clear if encryption and authentication would be required for all internet-connected RE or only for specific product groups. However, such technical solutions were seen as being able to address 80-90% of problems, and some costs data was obtained.
5. It is not presently clear whether economic operators would be able to re-use testing results to ensure compliance with other EU legislation to demonstrate compliance with the RED. Examples in this regard are:
    a. The management of business processes relating to data protection by design and default under the GDPR. It was seen as unclear at this stage until the text is drafted as to how the requirements in the DA on Art. 3(3)(e) would differ from those under Art. 24 and Art. 25 of the GDPR.

   b. Participating in a (voluntary) product-specific CSA certification scheme. There were concerns that the testing requirements for a certification scheme may differ from those adopted in harmonised technical standards, and the risk of additional testing costs being incurred.

   c. Whether internal testing by manufacturers against existing industry standards (including standards individual firms have developed) would be sufficient, or whether internet-connected RE would need to be retested.

6. Whether third-party conformity assessment would be mandatory, or only for products identified as being 'high-risk' (see the categorisation of risks by product type in Section 4.2 – synthesis assessment of security vulnerabilities).

7. Lastly, as regards the quantification of the costs of existing EU legislation (Option 0), although an effort was made to review the impact assessments for the GDPR and e-Privacy Regulation, the published IAs do not shed light on the costs of compliance for industry (see relevant sub-section).

Existing technical standards typically address cybersecurity in a broader sense by preventing online device penetration, which would help to achieve the desired regulatory objectives set out in Art. 3(3)(e) and Art. 3(3)(f). This was confirmed in the mapping of technical standards to identify potential technical solutions that could be used to develop harmonised EN standards in future carried out by CEN/ CENELEC and ETSI (see Section 4.2.3). As a result of implementing such technical standards, however, even if data protection and privacy and protection from fraud are not explicitly in focus, a consequence of better protecting devices through improved security is that data would be protected, and privacy not compromised and fraud prevented. This corresponds with the conceptual framework outlined in Section 3.2. Industry was therefore unsure what the costs of compliance are likely to be, as it not yet clear what types of baseline security requirements might be introduced, and from a CBA perspective, how the costs of strengthening cybersecurity generally could be disentangled from the specific costs associated with strengthening data protection and privacy and protection from fraud, which are a sub-set of a wider range of issues that could be tackled through cybersecurity measures.

ESOs and manufacturers interviewed commented that there are currently a lack of technical standards that specifically focus on data protection and privacy and protection from fraud (for the latter, other than security standards for payments). This was also confirmed in our assessment of technical solutions through the desk research (see Section 4.2.3).

It was possible to partially overcome the above-mentioned quantification challenges, by:

- Undertaking an assessment of technical solutions that are already available (see Section 4.2.3);
- Reviewing good practice guidance produced by ENISA setting out minimum baseline security requirements [159] similar requirements developed by NIST and other available developments such as ETSI standard TS 103 645 on consumer IoT security. These provide an indication as to what baseline security requirements might look like, and have been factored into the CBA.
- Gathering selected examples of compliance costs through product case studies as to the amount of time involved and the costs associated with the testing of internet-connected RE and wearable RE to ensure minimum baseline security functionality, such as to strengthen data protection and privacy and to provide adequate safeguards for protection from fraud;
- Obtaining qualitative feedback from manufacturers and other economic operators, national authorities and MSAs on issues, such as:
    - The main cost drivers involved in strengthening the security of internet-connected RE,

[159] Baseline Security Recommendations for IoT Security (in the context of Critical Information Infrastructures), ENISA - https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

differentiating between administrative and substantive compliance costs;

- The extent to which there are likely to be 'Business as Usual' (BaU) costs for producers (costs that would be incurred anyway regardless). For example, the extent to which technical solutions are already being used by manufacturers to strengthen product security was reviewed. This has helped to provide the basis for the development of working assumptions regarding the nature and magnitude of any additional costs over and above compliance costs relating to existing EU legislation.
- How far producers of internet-connected RE may already be incorporating data protection by design and default into their business processes as part of GDPR compliance. As the concept of security by design and default is an extension of this existing legal obligation, this could reduce the net costs as there would be high BaU costs.
- How far even if there were not a regulatory approach, costs would still be incurred anyway by producers and other economic operators involved in global value chains (GVCs), for example due to risk and reputational management reasons.

5.3.3 Compliance costs types

It is important to define the different types of costs under examination in this impact assessment. A distinction can be made between 1) administrative costs incurred by economic operators and 2) administrative burdens incurred by regulatory authorities and market surveillance authorities (MSAs) to check compliance, carry out monitoring and enforcement activities, including product testing to check compliance levels.

A further distinction can be made in the case of the costs for economic operators between:

- **Administrative compliance costs** associated with carrying out various information obligations relating to administrative requirements that would be required were one (or both) of the delegated acts to be activated. Examples are: updating the declaration of conformity (DoC), preparing a technical file to support the DoC, carrying out testing and conformity assessment procedures by the manufacturer, or by a third-party on a voluntary basis, etc.
- **Substantive compliance costs -** R&D&I and engineering costs relating to the redesign of existing, and / or new product development to ensure that internet-connected RE products incorporate security considerations prior to being placed on the market in a way that would protect users by ensuring adequate safeguards for data protection and privacy and protection from fraud.

Examples of substantive compliance costs are final manufacturers ensuring in the procurement process that chips integrated into internet-connected RE integrates secure authentication and encryption technologies. Embedding security by design and default principles into the manufacturing process from the outset may help to reduce substantive costs as this would avoid costly re-engineering for products already on the market to ensure that they are RED-compliant (if Art. 3(3)(e) were to be activated).

A distinction can also be made between the:

- **Direct costs** of compliance if the activation of the two delegated acts (Art. 3(3)(e) and Art. 3(3)(f)) went ahead. Under Options 2, 3 and 4, direct costs for manufacturers would be incurred to comply with (minimum) baseline security requirements for internet-connected RE. A discount to reflect Business as Usual costs should be made to reflect the costs of compliance with existing EU legislation such as the GDPR, the ePD and the (voluntary) Cybersecurity Act under Option 0.
- **Indirect costs** – may also be generated as a result of new legislative requirements being introduced, for instance, those incurred by companies upstream in the value chain, and passed on to users through a higher price for inputs (e.g. components integrating higher levels of encryption,

and any knock-on costs, such as ensuring compatibility with the hardware). Indirect costs are also related to opportunity costs, for instance, delays in time to market due to additional testing and compliance processes.

Other issues relating to the costs of compliance considered are:

- **Differences in regulatory compliance costs (Options 2, 3 and 4) depending on firm size, e.g. SMEs compared with large firms.**
- The extent to which **compliance costs vary as a percentage of the total costs of manufacturing,** depending on the types of internet-connected RE in question, and on the volume of products being sold. The compliance costs for high-volume products can be spread across mass production, whereas the costs for more specialist or low-volume products cannot be.
- **The costs of non-action.** There could be economic costs due to non-action, if the security of internet-connected RE is not improved, for instance, sub-optimal take up and adoption of the industrial and consumer IoT due to lack of trust among users of such equipment. A further risk is that of undermining the full potential of the European Digital Single Market, and the potential of internet-connected RE to speed up digital transformation of the European economy and society.

5.3.4 Quantification of the costs and benefits of existing EU legislation (Option 0)

An effort was made to quantify the costs of existing EU legislation (Option 0), as this already provides at least some safeguards as regards data protection and privacy through the GDPR, the e-PD and the proposed e-PR. In particular, the impact assessments were consulted, where these existed. The main challenges are that:

- Only the executive summary of the impact assessment for the GDPR (2012) was available, rather than the detailed workings. Even had the detail been available, any costs estimates tend to focus on compliance costs for all types of organisations (e.g. of having a DPO in place, implementing GDPR compliance organise-wide etc.). The IA does not focus on the costs for industry of implementing relevant Articles such as Art. 24 and 25.
- The e-Privacy Directive (2002) was adopted before the requirement to undertake an impact assessment was introduced (2006). Whilst there is a full IA (in SWD format) available for the proposal for an e-Privacy Regulation (2017), much of the quantification focuses on the costs of cookies on websites, and on extending confidentiality requirements to over-the top ("OTT") services that were previously unregulated compared with regular telecoms providers. There does not however appear to be any quantification of the costs of the e-PR for industry.

Therefore, in the absence of data, we have relied on the limited secondary literature available. A report to quantify the benefits arising from personal data rights under the GDPR was carried out by London Economics [160] in 2017. This helps to quantify the economic impacts of a lack of data protection. A lack of data protection is known to cause detriments, ranging from *"costs incurred [by firms] when data is breached or misused, or collected in ways that consumers deem too intrusive" and identity theft, price discrimination, stigma or psychological discomfort for consumers. Benefits turn into opportunity costs when individuals refrain from disclosing personal data. Disclosure (and non-disclosure) can also cause positive and negative externalities (social benefits/costs greater than the benefits/costs to an individual or firm involved in the transaction).* [161]

[160] Research and analysis to quantify the benefits arising from personal data rights under the GDPR, London Economics, May 2017, Report to the Department for Culture, Media & Sport https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/635701/PersonalDataRights_LE_-_for_Data_Protection_Bill__1_.pdf

[161] Acquisiti et al. (2016), Tamir and Mitchell (2012), Stone and Stone (1990) and Feri et al. (2016).

5.3.5 Stakeholder feedback on the costs of activating the delegated acts

Stakeholder feedback on costs and cost drivers has been gathered through the interview programme and online surveys. The focus was on estimating the costs of the regulatory options, in particular on Options 2, 3 and 4.

The evidence base draws on: 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 RE, and interview feedback with circa 25 interviewees from a further 15 manufacturers carried out through the 6 product case studies (see Annex 8). In this section, we provide an analysis of the feedback received.

5.3.5.1 Administrative costs of compliance

Administrative costs relate to the compliance-related administrative tasks that need to be performed to ensure compliance with the law and to fulfil the required information obligations. In the case of the RED, if the DAs were to be activated, then economic operators (e.g. manufacturers of internet-connected RE, but also other economic operators in the value chain, such as electronic component manufacturers would need to comply with additional essential requirements pertaining to 1) data protection and privacy and 2) protection from fraud.

In order to develop a better understanding of potential administrative costs, a typology of such costs was developed, as per the following table:

Table 5.4: Typology of administrative costs

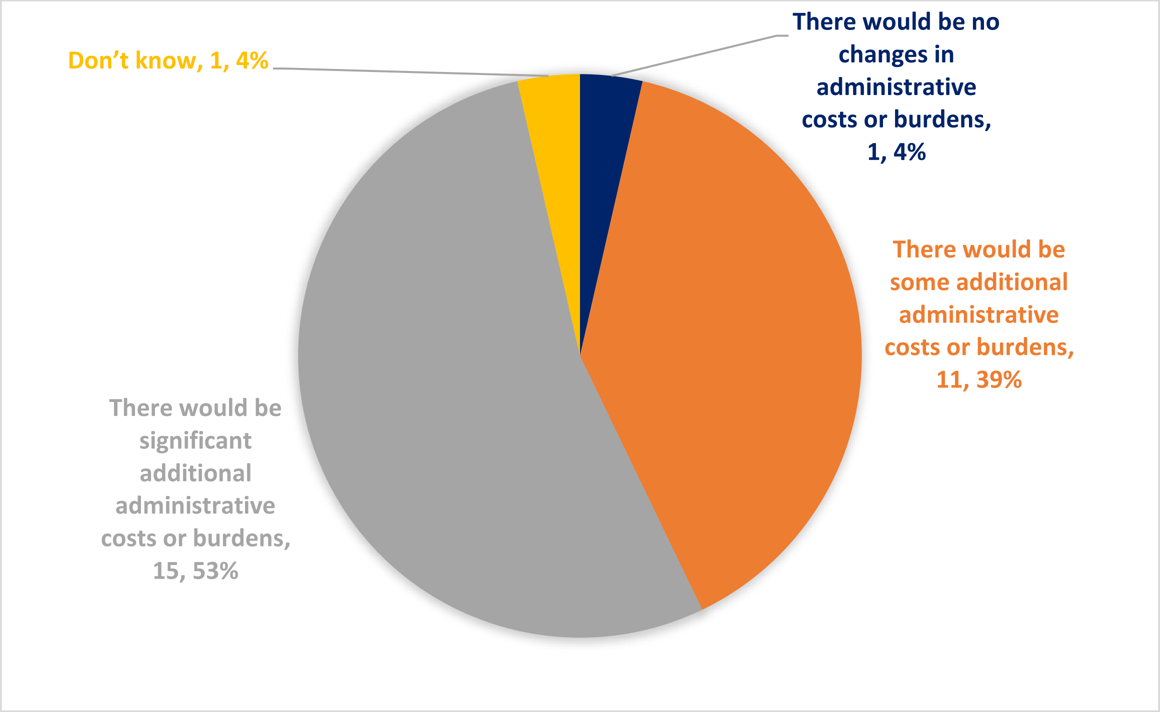
	Administrative costs
1)	Familiarisation with the essential requirements pertaining to 1) data protection and privacy and 2) protection from fraud, prior to placing products on the market
2)	Updating the Declaration of Conformity (DoC) to reflect the additional essential requirements.
3)	Updating the technical file to reflect any technical standards used to comply with the possible activation of Art. 3(3) (e) and / or 3(3) (f) pertaining to 1) data protection and privacy and 2) protection from fraud.
4)	Internal product testing and certification to demonstrate compliance with requirements relating to 1) data protection and privacy and 2) protection from fraud.
5)	(Voluntary) use of third-party product testing and certification to ensure compliance with any new essential requirements.

5.3.6 Administrative costs - online survey findings

Feedback was received from economic operators (EO) through the online survey (targeted consultations) 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 EO, and the survey cohort is therefore 28. Although this is a relatively low number, some manufacturers were from large global electrical equipment and household appliance manufacturers that employ tens of thousands of people. Moreover, the online survey responses have been triangulated against the feedback from interviews with manufacturers carried out as part of the product case studies.

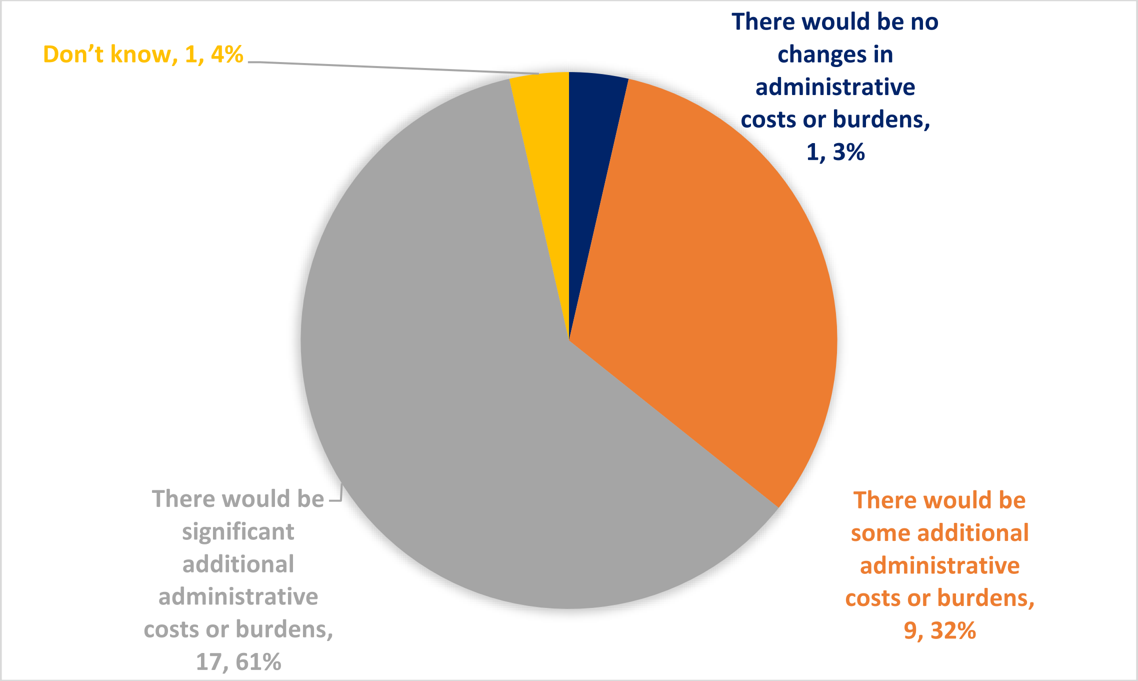
EO were almost unanimous in stating that there would be additional administrative costs or burdens related to new regulatory requirements on data protection and privacy and on protection from fraud.

Figure 5.1: Administrative burden of new regulatory requirements (data protection & privacy)



Source – targeted consultation, online survey

Figure 5.2: Administrative burden of new regulatory requirements (fraud)

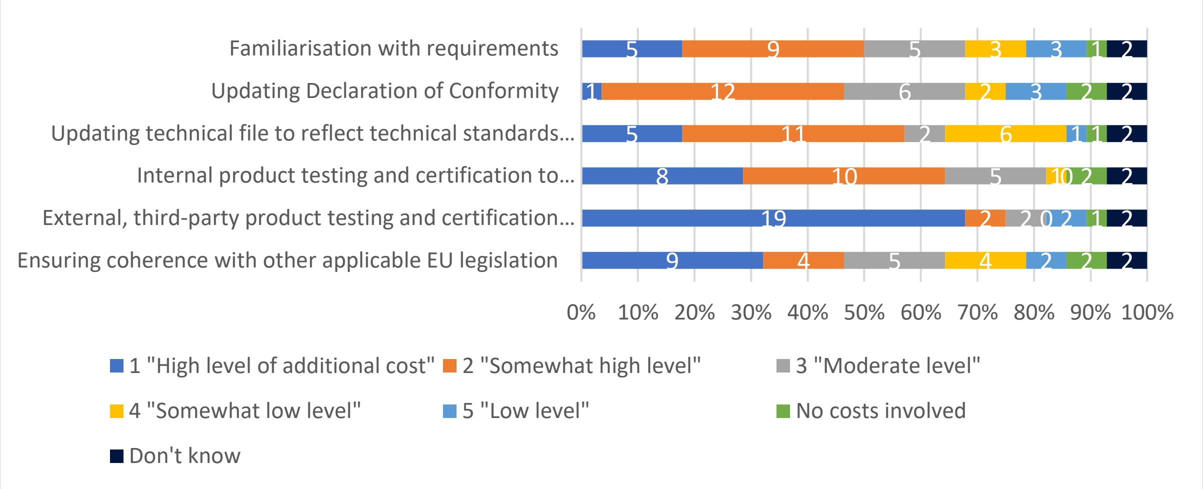


Source – targeted consultation, online survey

Respondents were also asked to comment on the type of administrative costs their firm would incur if one or more of the delegated acts under the RED pertaining to data protection and privacy and protection from fraud were to be adopted. When asked to specify the nature of any "other" costs, respondents mentioned costs such as 1) the costs of different applicable legal acts, standards applicable and conformity assessment procedures 2) third-party certification costs; and 3) a lack of harmonised standards.

The firms that expected to incur each type of administrative cost were asked to comment on the level of such costs, as show in the figure below.

Figure 5.3: Types of administrative burden incurred by firms



Source – targeted consultation, online survey

The different types of administrative costs associated with compliance processes are now provided. 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 corroborated in the interview programme through discussions with industry stakeholders and individual manufacturers.

Table 5.5: Level of administrative cost associated with different compliance processes

	1 High	2 Somewhat high	3 Moderate	4 Somewhat low	5 Low	None
Familiarisation with requirements	18%	32%	18%	11%	11%	4%
Updating Declaration of Conformity	4%	43%	21%	7%	11%	7%
Updating technical file to reflect technical standards needed to comply with strengthened protections	18%	39%	7%	21%	4%	4%
Internal product testing and certification to demonstrate compliance	29%	36%	18%	4%	0%	7%
External, third-party product testing and certification to ensure compliance	68%	7%	7%	0%	7%	4%
Ensuring coherence with other applicable EU legislation	32%	14%	18%	14%	7%	7%

Source – targeted consultation, online survey

5.3.6.1 Interview feedback on administrative costs

Regarding quantitative data on costs, estimates of the order of magnitude of costs were gathered from industry associations and a limited number of individual manufacturers. Some information about the potential compliance costs, especially under possible future regulatory scenarios, are provided in the product-based case studies (see Annex 8). Selected examples of cost drivers from the case studies are provided in this section.

An example of the potential costs of activating the DAs was received from a lawnmower association via their umbrella association. The estimated costs of requiring encryption and authentication, two of the main ways in which many internet-connected RE and wearable RE could be secured, are in focus:

Box 5.3: Case study - The administrative and substantive costs of compliance of integrating cybersecurity requirements into connected IoT products: the case of lawn mowers.

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.

Description of RED-relevant industry changes in past 5-10 years: lawnmowers have traditionally been an offline simple product subject to core industrial product legislation, such as the LVD and the EMC. 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[162]. 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 introduced relating to data protection and privacy for lawnmowers. It was estimated that:

- Administrative compliance costs were estimated at 25,000 EUR per product.

[162] See selected industry examples such as from Bosch https://venturebeat.com/2019/01/07/bosch-details-connected-robot-lawnmower-gesture-sensing-kitchen-projector/ and Belrobotics https://www.belrobotics.com/en/mowers/bigmow-connected-line/

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

- 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 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 dominant market players are both European and global. There were concerns that European manufacturers might be at a competitive disadvantage 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.

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

5.3.6.2 Cost of testing - third-party conformity assessment and internal testing

In this sub-section, the costs of internal testing and third-party conformity assessment in relation to internet-connected RE and wearable RE are considered. Testing costs to check compliance with the essential requirements is one of the major areas of costs associated with compliance with the existing essential requirements of the RED.

It is not yet known whether mandatory third-party conformity assessment would be needed if the DAs were to be activated to check for baseline security requirements. As with the existing essential requirements, it is possible that third-party testing would be non-mandatory, unless a particular category of internet-connected RE or wearable RE posed a particular risk. Nonetheless, many manufacturers (especially SMEs) use third-party testing of products against harmonised technical standards regardless as to whether these are mandatory as they do not have in-house testing laboratories.

The following stakeholder feedback was provided in relation to testing costs:

- Testing costs would be incurred by manufacturers to check that their products were compliant with the RED's existing essential requirements to include baseline security requirements.
- Manufacturers viewed it as being impossible to disaggregate the costs of testing security features specifically pertaining to data protection, privacy and fraud as they saw safeguarding device-level security as being part of engineering-in cybersecurity features to prevent device penetration, and

not something that could easily be disentangled from the specific aspects of security mentioned in Art. 3(3)(e) and Art. 3(3)(f).

- Manufacturers had some difficulty in understanding what specific steps they would need to take to ensure protection from fraud and what this would mean from a testing perspective. Therefore, quantifying the specific costs of putting in place protection against fraud was seen as not possible, without further guidance on what types of technical standards are envisaged. Payments fraud was however an exceptions, as the types of steps necessary to prevent fraud were better understood in terms of technical solutions.
- Some data on testing costs was nevertheless obtained (see subsequent table). A key finding was that internal and especially external testing are the most costly type of administrative costs.
- There are two aspects to analysing testing costs, the total costs of testing and the costs per unit. Internet-connected RE produced in high-volume can spread the testing costs across many different products compared with low-volume/ niche-products. The production volume impacts the level of risk, and in turn the related testing costs.
- 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 RE may find it challenging to cover the costs as unit cost testing is high. Smart alarms were cited as an example where the sector is dominated by many SMEs producing different models of smart alarms in low volume. A concern raised was that the compliance costs may disproportionately affect such producers.
- The location where internet-connected RE and/ or wearable RE will be used impacts on the assessment of the level of risk, the likelihood of the risk materialising and the impact of device penetration and data loss. This in turn will influence the level of testing costs. Internet-connected RE likely to be used in environments requiring higher levels of security, will therefore need to be tested to a higher level of security – beyond baseline security requirements - than would be the case if they were only intended to be used in a low-risk environment.
- Taking a smart thermometer as an example, the same product when used in a critical infrastructure environment poses a higher level of risk compared with when the product is connected to a home network. A security research expert mentioned that higher testing costs will be incurred if there are higher than average risk levels associated with either the intended location of usage or the product’s technical characteristics.

Examples of the **costs of third-party testing for checking product security** are now provided. Whilst many manufacturers found it difficult to provide any estimates, some data was provided, as per the table on the follow page:

Table 5.6: Examples of the costs of third-party testing for economic operators

Type of internet-connected RE product	Estimated costs (and any notes)	BaU costs	BaU rationale	Number of days of testing	Source(s)
• **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).	• 1-2 days • • 5-10 days •	• Interviews with industry associations and manufacturers
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	• Interviewee with a testing lab
• **Simple and complex internet-connected RE**	• 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	• Costs data shared by parallel software study on Art. 3(3)(i)
• **Complex internet-connected RE**	• 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	• Costs data shared by parallel software study on Art. 3(3)(i)
• **Complex internet-connected RE products (with extensive software)**	• Total costs, EUR 170,000. Internal costs • 4 software engineers – €60,000/ year X 6 months development cost = €120,000. External costs • EUR 50,000 lines for checking software code of more complex internet-connected RE products. • One quarter of the costs were direct	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)	• Costs data shared by parallel software study on Art. 3(3)(i)

Type of internet-connected RE product	Estimated costs (and any notes)	BaU costs	BaU rationale	Number of days of testing	Source(s)
	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				
• **Routers - example**	• C.a. 129,000 EUR 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	• Interview with manufacturer of internet-connected RE
Wearable RE example	• >35,700 EUR • Combination of internal and external testing costs.		• Estimation from a wide range of data from across the studies and interviews	1-2 months	• Interview with manufacturer of internet-connected RE
Testing garden equipment	• 20,000 - 25,000 EUR 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	• Interview with EU industry association following consultation with garden equipment stakeholder.

The data obtained shows that there are some variations in estimated testing costs, although a consensus that the costs per product are likely to be in the order of:

- EUR 5,000 – 15,000 for simple RE products;
- EUR 20,000 - 30,000 for more complex products; and
- >EUR 50,000 for heavily software-dependent internet-connected RE.

Only limited examples of product-specific testing costs to meet minimum baseline security requirements were identified, for instance for routers and lawnmowers. A few generalisations were made regarding the estimated testing costs of simple internet-connected RE, which take a lot less time to test and would incur much lower testing costs than complex RE.

An interviewee from a testing body highlighted that costs vary as testing bodies commonly offer service packages, and the price will also depend on the level of security required for the given product. It was estimated that testing for (minimum) baseline security requirements for a simple product implies a minimum of one-two days testing and might cost around 5,000 EUR. Conversely, testing for high-level security requirements for complex products may involve months of testing. It may sometimes require a combination of internal testing and third-party validation. Total testing costs will therefore vary greatly depending on 1) the category of internet-connected RE concerned 2) the nature of the security requirement(s) and 3) whether the product is heavily dependent on software (see below).

There were also some outliers in the costs estimates, such as a laboratory that suggested it would take one month to test a simple piece of internet-connected RE, and an estimated cost of EUR 30,000-40,000. This was higher than other estimates received from manufacturers and from MSAs. This suggests that testing costs vary greatly depending on the specific product type, country and the availability of suitable laboratories to carry out such testing. Some interviewees (from MSAs and industry associations) pointed to a lack of adequate number of testing houses to carry out security testing of internet-connected RE, and the need for training and capacity-building, as cybersecurity requires specialist expertise. In countries with a lower number of suitably-qualified testing bodies, there is a risk that testing costs might be higher, at least initially.

Checking software was found to be very costly. However, estimating compliance costs involving testing on a disaggregated basis was found to be very difficult, as testing is already carried out regardless of regulatory requirements by manufacturers themselves. This tests for a product's functionality and for other aspects of its performance and security aspects. A more detailed example from the routers product case study is now presented, which highlights how some costs would be incurred anyway regardless as to whether the delegated acts are activated (pointing to high BaU costs).

Table 5.7: Routers - case study showing estimated costs of security testing prior to product launch (current situation)

Headings	Description
Product group:	Routers
Market size/ structure:	The current global market for routers is expected to grow at a Compound Annual Growth Rate (CAGR) of 16.9% over the next five years, and will grow from 810 million US$ in 2019 to 2070 million US$ in 2024. [163] 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 [164]

[163] Router Market 2019 Research report https://www.360researchreports.com/enquiry/request-sample/13814132

[164] Source - global industry analysts. https://www.strategyr.com/MCP-1750.asp

Headings	Description
	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-enabled RE devices, an expansion in industrial and consumer IoT and in cloud-based networking.
Type of costs:	Internal and **e**xternal 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 FTE 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 QA 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 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.

Headings	Description
	- 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 RE 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 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: CSES – analysis of results from interview programme, desk research, and data estimates on market size/ structure (latter from Tech4i2).

It was pointed out that there may be **differentiated costs for SMEs and large firms.** Some SMEs maintain a large product catalogue, but in low volume. If they have to pay for an average of say 5 days' testing per product but produce many products overall, they would incur quite high costs. An unintended consequence could be the risk of SMEs deciding to reduce their product range in future. However, this would also depend on how the DAs are implemented. A means of reducing the costs for SMEs would be to draw up the DAs in a way that considers how far testing already carried out could be used to demonstrate compliance with future harmonised technical standards, where existing standards are similar and would allow this.

Larger firms are better able to spread compliance costs and risks across many products. They commonly also have the laboratory infrastructure, engineers and product compliance staff to carry out in-house testing. In parallel, larger firms are more likely to carry out both internal and external third-party testing of their products, which means increased compliance costs. This would help to mitigate the risks of security breaches.

A crucial variable influencing compliance costs for SMEs and large firms is **whether they need to carry out third-party testing.** If they incorporate basic security features from the design phase into the design of internet-connected RE, and implement security by design and default practices, this may negate the need for additional third-party testing. However, this would depend on the type of internet-connected RE, the level of risk associated with the product and the specific security features required in Technical Standards pertaining to baseline security requirements.

A general observation made by manufacturers in relation to the compliance costs of extending the RED's existing essential requirements is that some economic operators, especially from Asia, may be non-compliant with the existing essential requirements. It was therefore suggested that such manufacturers are unlikely to take the necessary steps to be compliant with any new, additional essential requirements introduced through the activation of the two DAs. The level playing field argument was raised, as there were concerns among some industry associations that the additional costs will be faced by responsible manufacturers, rather than by non-compliant economic operators.

There were concerns among industry regarding **possible duplication of some aspects of administrative costs.** For instance, if a particular manufacturer decides to achieve compliance with a certification scheme under the CSA, they may be required to carry out additional testing, even for the same product, were requirements to be introduced through the RED. Although manufacturers did not believe they would have to redesign the internet-connected RE, they may have to re-test their product to ensure they meet any new technical standards developed to achieve RED compliance, for instance if a new standardisation mandate were to be issued by ETSI relating to Art. 3(3)(e) and 3(3)(f).

Some cost benchmarks were also identified pertaining to ensuring security in other relevant EU legislation. For example, whilst the Cybersecurity Act (CSA) is a voluntary scheme, some manufacturers view the scheme as being "*de facto* mandatory", as their customers will expect them to meet the certification requirements if these are rolled out in a particular product category. Moreover, the costs of achieving certification were seen as being quite high, although there were also seen to be marketing benefits in being able to export to third countries, for instance using a European cybersecurity label. According to an industry association, the costs of testing one device for a certification scheme is about 40,000 EUR. Therefore, manufacturers and industry associations stressed the importance that if the Commission did activate Art. 3(3)(e) and 3(3)(f), it would be helpful to ensure coherence between the CSA certification schemes, associated testing and harmonised EN standards. However, some industry stakeholders thought that this would be very difficult in practice, as testing against a set of new harmonised EN standards (pertaining to security under the RED) would require a new set of testing results.

A general observation made by manufacturers in relation to the costs of compliance of extending the RED's existing essential requirements is that some economic operators, especially Asian manufacturers producing unbranded products, are not yet fully compliant with the existing essential requirements. However, this relates to manufacturers selling cheap products and it should be stressed that there were also found to be many responsible manufacturers who take compliance with EU industrial product legislation (including the RED) seriously. It was suggested that manufacturers not yet RED-compliance are unlikely to invest in demonstrating compliance with additional essential requirements introduced through the activation of DAs regarding safeguards to ensure improved security (data protection and privacy, protection from fraud). The level playing field argument was raised by some European manufacturers, as the additional costs will be experienced by responsible manufacturers, and other economic operators in their value chain.

5.3.7 Administrative burdens

Administrative burdens are defined as the additional cost of fulfilling information obligations to public authorities (or to other third parties), as required by the legislation. Any potential administrative burdens from activating the two DAs from the perspective of **market surveillance authorities (MSAs)** have also been considered. If baseline security requirements were to be introduced through the newly-activated DAs, MSAs would need to actively monitor and enforce their effective implementation. This would imply costs linked to testing internet-connected RE and costs linked to checking compliance documentation, such as technical files produced by manufacturers.

Approximately 10 MSAs were interviewed, and further MSAs were consulted through the online surveys. The study team also interviewed and discussed with MSAs at three consecutive RE EG meetings. Some MSAs mentioned that they test internet-connected RE devices and products themselves, and that typically, this might involve a couple of days of testing to check whether the RE concerned is compliant with the essential requirements.

In such instances, some costs would be incurred, estimated at circa EUR 5,000 – 10,000 for simple equipment, and up to EUR 20,000 for more complex equipment. However, these would not be prohibitive. It was noted that presently, most MSAs do not have much direct experience in checking and testing the security of internet-connected RE, as they have been focusing to date on checking the safety requirements. Therefore, many MSAs found it difficult to quantify costs, as these are activities they are not yet undertaking. Moreover, they would need to develop technical capacity before they are able to carry out such testing. Expertise could however be brought in from externally. For instance, an MSA from Germany mentioned that to check compliance with the essential requirements of existing industrial product legislation, they use a third-party testing house. Examples of costs are provided below:

Table 5.8: Examples of the costs of testing for market surveillance authorities to test internet-connected RE devices and products

Type of internet-connected RE product	Estimated costs	Number of days of testing	Source(s)
Outsourcing by an MSA to a third-party testing house	10,000 EUR	5 days	Interviewee with a testing body and with a national regulatory authority and MSA that outsources testing

The research found that under a regulatory scenario, testing costs would vary depending which minimum baseline security requirements are introduced across different internet-connected RE and wearable RE. An interviewee from an ESO mentioned that they anticipated that checking compliance with such requirements would involve MSAs checking documentation as this would help to demonstrate through the mapping of business processes by manufacturers what steps had been taken to put in place security safeguards to ensure data protection and privacy, and protection from fraud.

Overall, the administrative costs were found to be proportionate to the benefits, with a high level of BaU costs of some 60-70%. However, the level of BaU is strongly dependent on how the technical standards are developed, how similar they are to existing industry and international standards, and whether retesting is required or existing testing results could be used to demonstration conformity with EN standards.

5.3.8 Substantive compliance costs

The substantive costs of compliance were also analysed. These include the potential costs of redesigning some products, were mandatory regulation to be introduced in instances where the IoT products / devices concerned would otherwise be non-compliant.

5.3.8.1 Substantive costs of implementing existing EU legislative requirements

There are already some substantive costs of implementing existing EU legislative requirements, such as Article 25 GDPR (data protection by design and default). This requires data controllers to put in place measures to assess the technical and economic feasibility of data protection by design and default. It was pointed out by the Commission (Unit dealing with the GDPR at DG Justice that the GDPR incorporates flexibility so as to ensure that the compliance costs are proportionate. For example, Art. 25 (mentioned above) and Art. 24 (technical and organisational measures to ensure that data protection and privacy are considered from the outset) are applicable to manufacturers if they are intending to collect any personal data as they fall under the GDPR as data controllers. However, requirements are not forced on data controllers prior to technical solutions being made available.

According to the desk research, *"data controllers will not be confronted with unreasonably costly requirements or with an obligation to integrate requirements for which no technical solution has yet been developed"*[165]. They would however be required to implement available technical solutions if the cost is not prohibitive. "*Once technical solutions for particular legal obligations are on the market at a reasonable price, data controllers will have to use them or implement their own equivalent or better solutions. This should create the middle ground for developers of data protection by design and default technologies, thus stimulating innovation in the market for technical DPbD solutions"*[166].

As not evaluation has been carried out of the GDPR, there is little information as regards how costly implementing particular articles of the GDPR is for industry. However, there is some literature that is beginning to consider this subject, though not specifically for industry manufacturers, and more for business generally. The cost of compliance with privacy requirements was seen as being more than financial, as ensuring continuous compliance is firstly an ongoing rather than a one-off cost, and secondly, is considered rarely scalable. A further issue for international manufacturers is that over time, GDPR-type regulatory regimes are emerging internationally, e.g. in California in the US, and global manufacturers are therefore increasingly required to comply with more than one data protection and privacy regime.[167]

5.3.8.2 Substantive costs – implementing the two delegated acts (Art. 3(3(e) and Art. 3(3(f)

Substantive compliance costs of implementing the two delegated acts (Art. 3(3(e) and Art. 3(3(f) were also considered. These are the costs that would be incurred if the two DAs were to be activated from product redesign and reengineering if manufacturers had to make any changes to products, either in the product design stage, manufacturing processes or retrospectively, by modifying an existing product to ensure that future products placed on the market were compliant.

Before outlining the qualitative findings based on interview feedback, the findings from the targeted online survey are first presented. Among economic operators responding to this question, 78% 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.

As regards research and development costs, two German manufacturers operating internationally believed that the extent of substantive compliance costs would depend on whether existing security features already incorporated into internet-connected RE would be sufficient to meet any new legal requirements. The possibility of having to undertake additional testing to check compliance with harmonised standards was raised, even if products were already compliant in terms of integrating minimum basic security requirements.

[165] 2013, Data Protection by Design and Technology Neutral Law, Mireille Hildebrandt, Radboud University Nijmegen, Laura Tielemans, Vrije Universiteit Brussel
[166] Idem
[167] https://www.cpomagazine.com/data-protection/understanding-the-gdpr-cost-of-continuous-compliance/

A micro-enterprise operating internationally reported that additional substantive compliance costs would affect the whole manufacturing and supply chain (e.g. including marketing materials), not just research and development costs. Three respondents stated that they could not comment on substantive compliance costs without knowing the details of any new requirements. One body representing associations of manufacturers suggested that new requirements within the RED would make the evaluation and tests more complex compared to an assessment under a horizontal regulation.

Figure 5.4: Incidence of substantive compliance costs

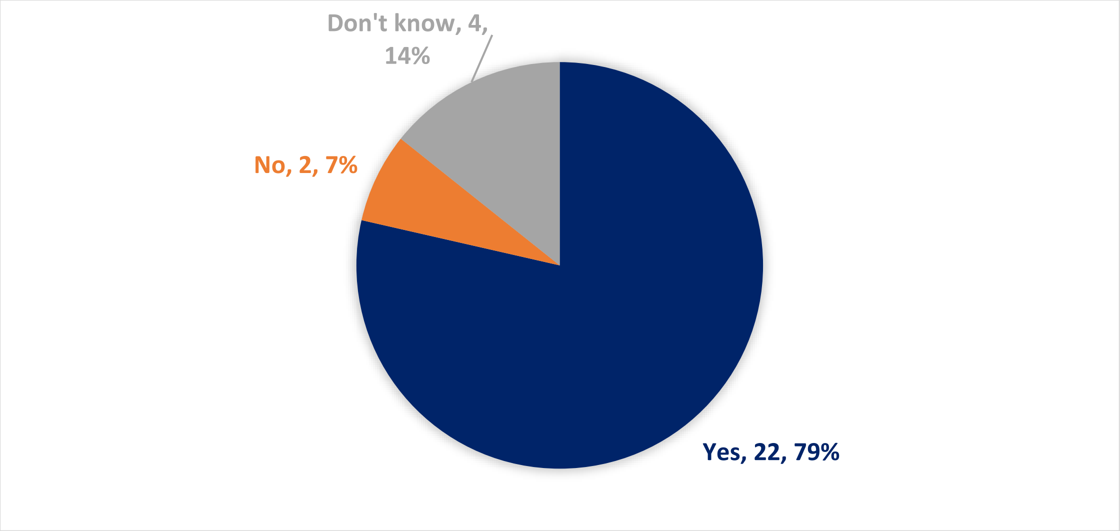


Figure 5.5: Research and development costs to redesign chipsets or components

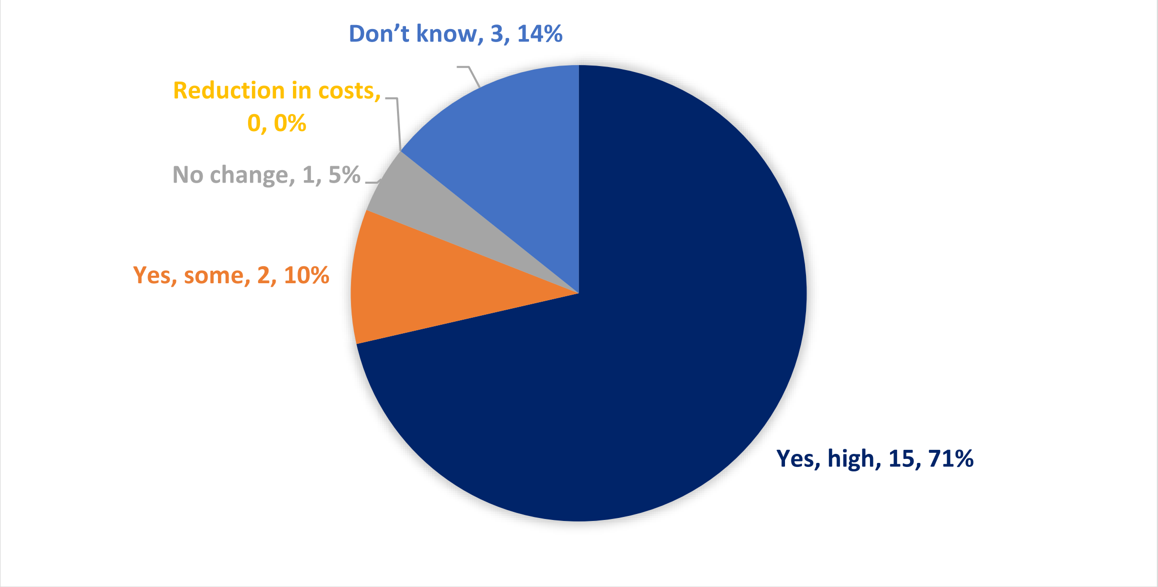
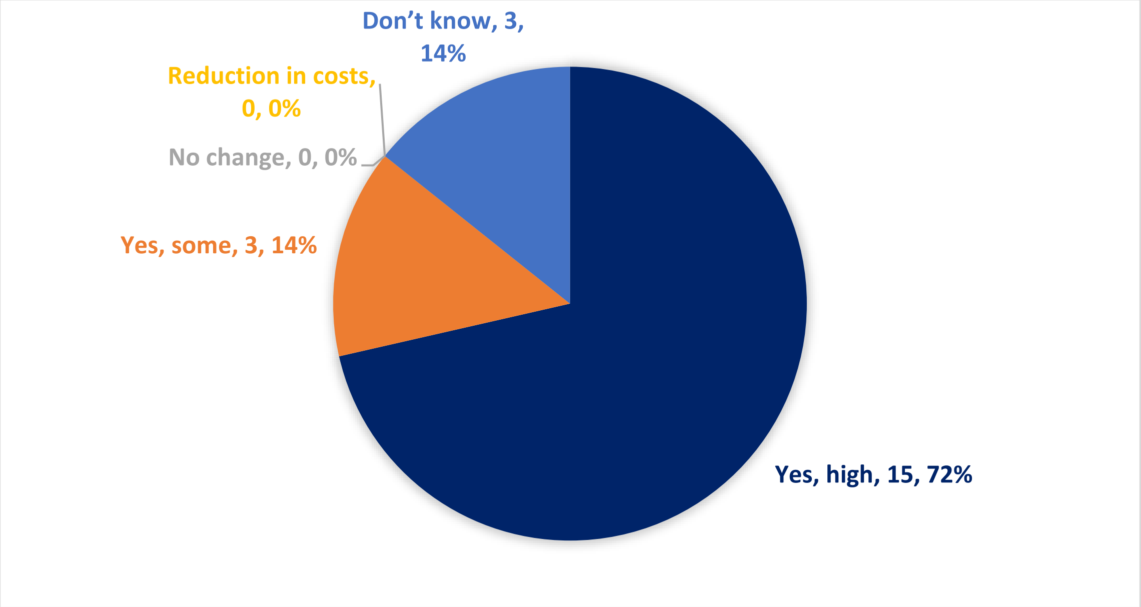


Figure 5.6: Research and development costs to redesign products



The findings as regards potential substantive costs if the two DAs were to go ahead based on interviews are that:

- Implementing minimum baseline security requirements was not seen as that costly in terms of substantive costs by most manufacturers, as key principles relating to security by design and default are already being considered by responsible manufacturers, either due to existing EU legislative requirements or as ensuring a high level of security is seen as part of their value proposition.
- The findings from the product cases were that in many cases, responsible manufacturers are already considering their legal obligations at the product design stage, particularly in respect of data protection by design and default under the GDPR, but also the implications if the proposed updating of the e-PD into the e-PR.
- However, views diverged as many industry associations suggested that there would be high compliance costs . This is rather contradictory, in that many 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 (mainly by strengthening security to prevent device penetration).
- The actual level of costs will depend on how far the requirements set out in future harmonised technical standards are similar to, or go beyond, what is already being done voluntarily.
- Some industry associations were concerned about the high costs of encryption, were this to be made mandatory, especially for internet-connected RE that does not intend to collect much personal data (e.g. robotic lawnmowers, smart meters). However, other stakeholders pointed out that unless well-protected, personal data and information cab be used malevolently (e.g. data on somebody’s smart meter tells whether they are at home or on holiday.
- Many European manufacturers integrate security by design and default principles into product design already, and it is therefore unlikely that they will be required to re-design or re-engineer IoT products and devices.

Before presenting more detailed examples of substantive costs, we first present an overview of feedback received in the following table.

Table 5.9: Substantive compliance costs: making a product data-encrypted to ensure higher levels of data protection and privacy

Type of internet-connected RE product	Estimated costs	Estimated FTE Required	BaU %	Source(s)
Lawnmowers	3 EUR / unit more expensive compared with unsecured lawnmower product with cheap Wi-Fi connectivity. Integrated encryption into the CPU would require changes to the electronics and additional technical support. This could result in extra costs of up to 10 EUR/ unit.	NA	0%	Industry association
Wearable radio equipment and other radio equipment	12,000 EUR	3-4 person weeks of work	10	Manufacturer

There was limited feedback on estimates of substantive costs, as many interviewees from industry associations and manufacturers were unable to give any quantitative information. Rather, they expressed qualitative views on cost drivers. Selected examples of feedback made by economic operators in relation to substantive costs are now outlined.

A MSA made the remark that, should the DAs be activated, several stakeholders will be impacted in different ways: manufacturers will be impacted because they will be required to integrate security-compliant features in their products; and customers will also be impacted because the substantive costs of compliance incurred by manufacturers will be passed on to them. Nonetheless, they maintained that the net impact of mandatory baseline security requirements could lead to a reduction in cost overall, due to the minimisation of the current hidden costs of unsecure products remaining on the European single market that the integration of cybersecurity-compliant product features would ensure.

Whilst some stakeholders argued that there would be high substantive costs of compliance incurred by manufacturers and other stakeholders in the value chain should the DAs be activated, others argued that these would be low. In general, more remarks were made around low substantive costs of compliance than high ones by interviewees.

Stakeholders that expressed the view that the substantive costs of compliance were likely to be low 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. It should be noted that minimum baseline requirements may suffice for low-risk products; high-risk ones may require a higher level of security.

Additionally, some technical solutions could be implemented without incurring in extra costs, for example using one-way push communication systems (although these may not be easy to implement due to unfamiliarity of the market with said systems), or switching to using similar cost encrypted chips or other components that would be compliant with any mandatory cybersecurity requirements relating to data protection and privacy that are already available in the market. These could therefore be used when carrying out R&D. However, some stakeholders pointed out that the same objectives could be achieved without mandatory requirements under the RED, since compliant chip solutions are already available on the market. It was argued that one of the biggest challenges is less the presence (or absence) of regulatory requirements, but rather the importance of awareness-raising among manufacturers of the importance of cybersecurity to ensure data protection and privacy and protection from fraud. This implies changing their design, engineering and procurement processes to ensure that they use and procure secure chips, micro-processors and other electronic components in a way that ensures high levels of security in connected RE products and wearables, especially consumer IoT from the outset.

A manufacturer argued that the substantive costs of compliance related to investment in meeting mandatory cybersecurity requirements relating to data protection and privacy could be mitigated by the lower level of risk associated with costly data breaches. Some industry interviewees in the cybersecurity field also pointed to the role of product insurance for Wi-Fi devices with IP connectivity to mitigate the risks of data breaches. However, using product insurance to ensure that manufacturers are able to deal with the financial implications of data breaches would not be as effective as designing in cybersecurity into connected RE products from the outset. Moreover, the costs of product insurance would be passed on to consumers and thereby lead to increases in the price of the product. A by-product of the adoption of the GDPR has been an uptick in demand for cyber insurance due to the risks for firms of cyberattacks and SMEs being identified as especially vulnerable. [168]

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. This applied for example in the case of the lawnmower example (see earlier), for the smart alarms industry and for smart toys (for the latter, see case study).

An example of cost drivers and the extent of BaU costs is provided in the following box from the toys industry on smart toys. Whilst it wasn't possible for those interviewed to provide quantitative estimates, the qualitative feedback provides insights into the difficulties in capturing costs:

Box 5.4: 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 DAs 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 Art. 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 toy manufacturers are already integrating data protection and privacy considerations as part of their broader approach to integrating security by design and default principles.

Substantive costs may be partially mitigated by improvements in the development of successive generations of internet-connected RE devices and products. For example, security weaknesses identified in some smart

[168] Hiscox - Cyber Readiness Report, 2019. https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

toys have meant that basic security requirements have been designed in to the design of next generation smart toys.

Further feedback was received regarding the substantive costs of encryption and for any requirements in technical standards to be extremely careful to avoid being overly-prescriptive in specifying which type of encryption, as this could impose major costs on industry, as per the box below:

Box 5.5: The benefits and costs of encryption – avoiding a prescriptive approach to ensure costs are proportionate

Benefits of encryption:

"Encryption is important in mitigating the damage caused by data breaches, complying with privacy and data protection regulations, and preserving brand and reputation". [169]Encryption has a number of benefits as regards protecting the unauthorised penetration of internet-connected RE. It moreover helps those using RE 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. 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.

As regards the benefits, *"If an organization encrypts its data with a self-encrypting disk, it is removing the physical risk of theft or data loss. It may have many privileged users and processes that interact with its data, but ensuring that encryption removes the risk is crucial".* [170] However, the costs of encryption can be costly, for instance, the same article found that encrypting app's can be costly.

Existing technical solutions: There are many encryption solutions available on the market to protect internet-connected RE, ranging from chip encryption, through to hardware and encryption of data storage space, and software encryption programmes. Reference should be made to Section 4.2.3 on technical solutions.

As regards data transfer, security protocols such as SSL are used by some manufacturers of internet-connected RE and software / app's developers. However, this only encrypts data when sent electronically. It does not cover data stored on a device. *"As data is written to disk, whether it's stored for one minute or several years, it should be encrypted".* [171]

A limitation of many existing internet-connected RE is that they do not currently have the processing power to incorporate encryption. the implementation of security controls is not always feasible due to the inherent limitations of IoT devices, e.g. resource and computational power limitations that might prohibit the use and access control mechanisms, encryption, key management structures and certificate schemes. [172]

As encryption requirements would result in additional costs for industry, the availability of electrical components with encryption capabilities at reasonable cost will need to be factored into the elaboration of harmonised technical standards. An interviewee from a major manufacturer said that there can be sometimes be incompatibility problems between higher-grade secure chips and components. The rationale cited was that different industries use different security protocols, and there is consequently a need to be careful about requiring specific encryption capabilities especially in hardware. This could otherwise cause difficulties in terms of combining high-end chips with lower-capacity chips. This depends how much data processing speed and memory is needed.

[169] " https://www.zdnet.com/article/the-price-of-full-disk-encryption-232-per-user-per-year/

[170] https://www.darkreading.com/endpoint/privacy/faq-understanding-the-true-price-of-encryption/d/d-id/1204593

[171] https://www.wired.com/insights/2013/05/9-biggest-data-encryption-myths-busted-2/

[172] 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

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 RE products and devices that retail or wholesale at a relatively low price (bearing in mind the manufacturers' profit margin may be slim).

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,"* [173] 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. The costs of full disk encryption are 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 RE. 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 100,000 EUR, although this will depend heavily on the type of internet-connected RE in question. 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 extending this to internet-connected RE 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.

Some literature has addressed the subject, such as a white paper on the Costs of Two-Factor Authentication [174]. The paper advocates the concept of the Total Cost of Ownership (TCO) to calculate the costs of introducing such authentication, *"where a range of factors are scrutinised to determine the long-term cost of purchasing and maintaining an application. This "Real Cost" of owning a software application might include important criteria that are often overlooked, such as hardware replacement costs, impact on existing IT infrastructure, maintenance and support contracts, and product usability".*

The paper furthermore points out that "*For most two-factor authentication solutions available on the market, the initial cost of the solution ranges from about 33% of the total cost to as low as only 10%. Upfront purchase costs typically include the cost of tokens (hardware or software), cost of server licenses, and cost of the first year support. Vendors use different pricing models ranging from a bundling of all three costs into one price to separately charging for one or more of the above items. Annual support and maintenance of a two-factor authentication solution provides for technical support services, product enhancements, incremental upgrades, and software patches. A warranty on the hardware can be*

[173] https://www.zdnet.com/article/the-price-of-full-disk-encryption-232-per-user-per-year/ and http://www.winmagic.com/ponemonstudy

[174] The Real Cost of Ownership - https://mpa.co.nz/media/4410/twofactorauthenticationtherealcostofownership.pdf

another critical component". However, there are evidently benefits as regards strengthening protection of internet-connected RE.

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

There would be short-term costs of transitioning to ensuring that such products and devices are made more secure. This could potentially lead to both costs and benefits, costs linked to the use of encryption in electrical components used in hardware, which could serve as a barrier to bringing some types of low-value RE devices and products to market. However, the costs of chips and semi-conductors has 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, manufacturers and electronic components manufacturers.

Examples were also provided as to how manufacturers might avoid extra substantive costs by changing the culture of product design. Some industry stakeholders made the point that using one-way push communication systems could be a cost-effective way of making products secure (e.g. smart meters) without needing to invest significantly in enhancing cybersecurity. However, others pointed out that push-pull communications are an essential feature of many internet-connected RE devices and products, as manufacturers use the ability to gather information independently of the user to monitor usage (e.g. smart meter readings) and/ or the performance of some devices, and for example to carry out virtual servicing and maintenance, which are less costly than carrying out servicing in person.

5.3.9 Business as Usual (BaU) costs

Business as Usual (BaU) costs are the costs that manufacturers would incur anyway as part of their current business practices, whether these are driven by regulatory requirements (e.g. the GDPR, Art. 24 and Art. 25), or for non-regulatory reasons, such as risk mitigation and reputational management.

Stakeholders interviewed were asked about the extent to which they already consider security by design and default principles during product design, engineering and manufacturing processes. The assumption is that if considerable attention is already being given by manufacturers to ensuring the security of to internet-connected RE, then the (net) costs of compliance with any additional requirements would be offset through high BaU costs, which would mean that the gross estimated compliance costs can be discounted.

Stakeholders highlighted that a significant percentage of manufacturers of internet-connected RE have already been developing security features and have incorporated them into the design of their products on a voluntary basis partly as part of risk management processes to prevent reputational damage and also to comply with their data protection by design and default obligations under the GDPR.

Whilst many manufacturers responding to the survey as well as those interviewed pointed to potentially high administrative costs, at the same time, the activation of the DAs points to high BaU costs, i.e. costs that are likely to be incurred anyway, regardless of whether EU legislation is introduced. An example is from the routers case study, where the router manufacturer in the consumer products domain noted that as their main distribution channel is wholesale, their customer base consists of major national telecoms and internet providers who distribute routers to consumers. Such customers are demanding in respect of product performance and security features, which means that the firm incurs significant internal and external testing costs before products can be launched. Therefore, many of the administrative and substantive compliance costs that might be incurred due to the activation of the DAs under Art. 3(3)(e) and (f) would be mainly BaU, with the exception of any additional (re)testing required under harmonised standards.

Interview feedback found that many manufacturers, especially leading market participants that invest strongly in their brands already either meet minimum baseline security requirements or go beyond these. This assertion was made by several industry associations interviewed, and confirmed by many manufacturers. According to a security expert in the IoT, for example, a competitive advantage of many European manufacturers of internet-connected RE is that are security-savvy and have invested in developing security features in their products. Examples are companies that implement SSL and TLS protocols which are considered 'state of the art' security features in certain internet-connected RE.

A further point regarding BaU costs was that some stakeholders stated that the costs of ensuring that IoT devices are more secure need not be that costly. For instance, the costs of procuring secure chips with encryption capabilities were sometimes no different from unsecure chips, according to one interviewee from a manufacturer. It was therefore more a matter of raising awareness among IoT device and household appliance manufacturers about the need to redesign their procurement policies and to demand secure chips from their electronic components supplier base than experiencing additional costs.

It was also pointed out that whilst unsecure internet-connected RE remains a problem on the European market, many European and global manufacturers – especially large firms - already follow security by design and default principles, and make cybersecurity features part of their marketing strategies. For manufacturers already adhering to good practices in security by design and default, any additional compliance costs would be heavily mitigated by high BaU, which would reduce net costs.

Conversely, SMEs may lack the resources to invest in strengthening product and device security and third-party testing to ensure that safeguards for data protection and privacy, and protection from fraud are ensured. They would therefore expect lower BaU in many cases, and could face comparatively higher administrative (and sometimes also substantive) compliance costs.

A problem was identified by a number of industry stakeholders (some industry associations, individual manufacturers) that compliance costs may not fall on the regulator's intended target of irresponsible producers selling very low-cost products without any basic security requirements, but rather on responsible manufacturers who are already compliant with the existing essential requirements in the RED and in other applicable industrial product legislation. There was a concern among stakeholders that manufacturers compliant with the existing requirements under the RED will face the compliance costs whereas manufacturers from third countries that have placed low-cost, non-compliant products on the European market will continue to try to get away with selling such products, as MSAs lack the resources to ensure effective market surveillance and enforcement. This is not only a resourcing issue, but was seen by one industry commentator interviewed as being a *"game of cat and mouse in that some low-price, non-compliant manufacturers bring particular products to the market for only a short period of time, making it more difficult for MSAs to act".*

5.3.10Compliance costs for large firms and SMEs

Some stakeholders interviewed from industry acknowledged that there are likely to be somewhat differentiated compliance costs between large firms and SMEs, but the dynamics in terms of the drivers of differences in costs are common across industrial product legislation, and not specific to the RED, or to possible new essential requirements relating to 1) data protection and privacy and 2) protection from fraud. Among the issues raised were that:

- **Large firms are in a better position to absorb compliance costs than SMEs.** Some stakeholders pointed out that compliance costs for large firms producing particular RE products in large volumes are relatively low, since the administrative costs of compliance can be spread across many units, meaning that the cost per unit is low.
- However, 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 those internationally. For instance, manufacturers may have to produce

separate technical documentation and incur testing and / or certification costs to verify the security of internet-connected RE they produce in the EU, US, Japan etc. It was noted by a representative from the certification and testing industry 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.

- **SME manufacturers of connected radio equipment and other connected electrical equipment and mechanical machinery containing radio functionality**. A number of SMEs pointed to the problem that they produce RE products in small numbers, therefore the testing costs associated with complying with additional essential requirements relating to cybersecurity, specifically, 1) data protection and privacy and 2) protection from fraud, could be prohibitive in some cases and prevent products expected to be produced in small quantities from being brought to market. This was seen as being particularly the case for SMEs with a large product catalogue, but whom produced in small volume.
- There is a general problem that **many (but not all) SMEs lack awareness about cybersecurity in general, including security measures to ensure adequate data protection and fraud.** It may therefore be relatively costly for them to manage technical compliance, such as embedding encryption and authentication into their products. The interview feedback suggested that this was especially the case for producers selling in low volume and/ or low-price products. In such instances, integrating security features may carry comparatively high costs per unit.
- **Several interviewees noted that SMEs do not have access to in-house testing capabilities, unlike large firms and multinationals, who commonly have access to their own laboratories.** Therefore, they would face the additional testing costs of using a third-party testing house. If the use of third-party testing for internet-connected RE were to be voluntary, like the existing essential requirements pertaining to product safety and electromagnetic compatibility, with the Self Declaration of Conformity (SDoC) possible, many SMEs would still incur costs, as they would typically use a third-party testing body to check for compliance with a particular technical security standard.
- **Specialist producers of internet-connected radio equipment** potentially face similar issues as SMEs in that if they produce in low quantity, compliance costs are likely to be higher per unit. This may deter them from bringing some products to the market.

5.3.11The costs of data breaches

An assessment was carried out of the costs of data breaches focusing on data protection and privacy, and on protection from fraud.

The types of costs that are typically incurred as a result of data breaches by companies are:

- **Direct costs**
  - Fines issued by data protection authorities due to non-compliance with regulatory requirements under the GDPR.
  - Costs directly attributable to data breaches and post-breach activities to manage the fallout e.g. informing customers about personal data and information compromised, bringing in IT security specialists to rectify the problem and strengthen security and the litigation costs.
- **Indirect costs** – costs which arise as a result of the breach, such as:
  - **Reputational damage -** a data breach has negative effects on the company's reputation with consumers, suppliers and other businesses. Some aspects can be quantified, whereas others are intangible;

- **Loss of customers.** Some customers may decide to stop using the products or services of an organisation as a result of the data breach, or as a result of malpractice and non-GDPR compliance in terms of the types of data being collected and how this has been used.

In addition, consumers and businesses themselves face costs as a result of data breaches:

- **Direct costs -** money lost due to financial fraud, identity theft. Time involved in responding to being contacted by company informing them about data loss, checking bank accounts, changing log-in and password details.
- **Indirect costs** – economic and societal costs where confidence in the security of IoT devices is undermined by data breaches leading to data protection and privacy being compromised and/ or fraud taking place. Consumer detriment also extends to non-financial aspects e.g. anxiety and stress as a result of a data breach.

Selected examples of different types of costs and key issues raised in literature on the subject are now provided. It should be noted that the examples are from the costs of data breaches for companies generally, as it was not possible to identify examples of fines issued under the GDPR directly to manufacturers of internet-connected RE. Indeed, there have only been a limited number of fines to date, and none appear to have been issued to industrial producers.

Regarding **direct costs,** a company experiencing a data breach may be fined due to non-compliance with their regulatory requirements as a data controller under the GDPR. The fines are significant, up to €20 million, or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is greater. The future e-PR, still under revision by the co-legislator, is likely to align with the financial sanctions possible under the GDPR. Evidently, this is an incentive for manufacturers in their capacity as data controllers and other actors in the value chain (data processors), such as third-party service providers to treat Art. 25 (data protection by design and default) seriously from the outset to reduce the risk of non-compliance and being issued with a fine.

However, as the GDPR only came into effect in May 2018, the number of fines to date has been limited. Moreover, it will take time until a sufficient body of case law has been established to establish how effective the Directive has been, and for the extent to which fines and case law have served as a deterrent to industry to discontinue manufacturing unsecure internet-connected RE products and devices.

It is worth listing examples of fines issued under the GDPR[175]. It is noticeable that these fines relate more to how personal data is insufficiently securely stored by companies and not to the security of the devices themselves. Whilst there have been some 40-50 fines issued to date by national data protection authorities, the data suggests that only three relates to Art. 25 and the issue of data protection by design and by default, and a further case relating to Art 35 (Data Protection Impact Assessments). None of these relate to industry.

These are illustrated in the following table:

[175] This website provides information about fines issues by different national data protection authorities - https://www.enforcementtracker.com/

Table 5.10: Article 25 and 35, GDPR

Country National data protection authority responsible	Dates GDPR breach occurred	Fine amount (EUR)	Company/ organisation fined	Articles of GDPR	Type	Summary of case resulting in fine
Germany Data Protection Authority of Berlin	2019-10-30	14,500,000 [176]	Deutsche Wohnen SE	Art. 5 GDPR, Art. 25 GDPR	Non-compliance with general data processing principles	The company used an archiving system for the storage of personal data of tenants that did not provide for the possibility of removing data that was no longer required. Personal data of tenants were stored without checking whether storage was permissible or even necessary. It was therefore possible to access personal data of affected tenants which had been stored for years without this data still serving the purpose of its original collection. This involved data on the personal and financial circumstances of tenants, such as salary statements, self-disclosure forms, extracts from employment and training contracts, tax, social security and health insurance data as well as bank statements. In addition to sanctioning this structural violation, the Berlin data protection commissioner imposed further fines of between 6,000 and 17,000 euros on the company for the inadmissible storage of personal data of tenants in 15 specific individual cases. See the separate entry.
GREECE Hellenic Data Protection Authority (HDPA)	2019-10-07	200,000 [177]	Telecommunication Service Provider	Art. 5 (1) c) GDPR, Art. 25 GDPR	Non-compliance with general data processing principles.	A large number of customers were subject to telemarketing calls, although they had declared an opt-out for this. This was ignored due to technical errors
ROMANIA Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	2019-06-27	130,000 [178]	UNICREDIT BANK SA	Art. 25 (1) GDPR, Art. 5 (1) c) GDPR	Insufficient technical and organisational measures to ensure information security.	The fine was issued as a result of the failure to implement appropriate technical and organisational measures (related to (1) the determination of the processing means/operations, and (2) the integration the necessary safeguards) resulting in the online-disclosure of IDs and addresses (internal/ external transactions) of 337,042 data subjects to their respective beneficiary (between 25.05.2018 -10.12.2018).
Sweden Data Protection Authority of Sweden	2019-08-20	18,630 [179]	School in Skellefteå	Art. 5 (1) c) GDPR, Art. 9 GDPR, Art. 35 (Data Protection Impact Assessments) Art. 36 GDPR	Insufficient legal basis for data processing	A school in Sweden was using facial recognition technologies to check the attendance of pupils. Under Article 35, the controller must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, particularly if the processing uses new technologies, and, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons. The school did carry out a DPIA, however they were not able to demonstrate compliance with Art. 35. There were breaches of many other Articles too.

[176] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf

[177]http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=3,241,32,146,79,143,149,112

[178] https://www.dataprotection.ro/?page=Comunicat_Amenda_Unicredit&lang=ro

[179] Go to https://www.enforcementtracker.com/# then click Art. 35. Also see https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf

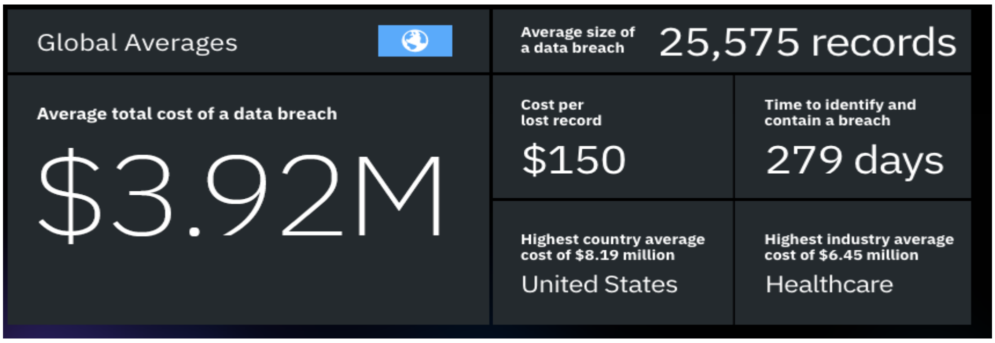
According to research carried out in 2018, *"one of the biggest impacts following a data breach is the effect on the company's reputation. Research has shown that up to a third of customers in retail, finance and healthcare will stop doing business with organisations that have been breached".* [180]

There are not only reputational issues to be concerned with, but also there are liability-related issues which mean that manufacturers collecting personal data should be concerned with ensuring GDPR compliance and building in data protection by design and default. Other types of costs incurred by companies include the **costs of litigation** due to personal data loss. These can be significant, depending on the number of personal data records accessed or hacked by an unauthorised third party.

Article 82 of the GDPR for instance states that *"Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."* This implies that there are already financial risks for manufacturers that go beyond the risks of incurring fines for non-compliance.

Regarding the **costs of data breaches**, this is very difficult to quantify an average, as the circumstances will vary. However, several pieces of research provide estimates for such costs. For example, in the US, IBM and the Ponemon Institute identified the average cost of a breach as $3.92 million in their 14th joint annual 2019 Cost of Data Breach study[181], though certain industries can have more costly breaches. The following infographic provides an overview of the order of magnitude of costs:

Figure 5.7: Average costs of data breaches globally – for companies



Global Averages

Average size of a data breach 25,575 records

Average total cost of a data breach

$3.92M

Cost per lost record

$150

Time to identify and contain a breach

279 days

Highest country average cost of $8.19 million

United States

Highest industry average cost of $6.45 million

Healthcare

Source: IBM Security and Ponemon Institute, 2019 Cost of a Data Breach Study

Among the high-level findings from the IBM / Ponemon study are that 1) The cost of a data breach extend beyond the fine itself 2) Breaches originating from malicious attacks are the most common, accounting for 51% of all breaches, 3) Smaller companies pay disproportionately larger costs in terms of costs/ staff member 4) Encryption has the greatest impact on reducing breach costs 5) Putting in place an incident response team and plan can lead to cost-savings and 6) Data breaches are most expensive in the US (due to greater litigation) and in the health care sector.

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 Internet of Things (IoT) devices. A key finding was that extensive use of IoT devices by organisations increased the risks.

A report from Juniper Research[182] found that the cost of data breaches will rise 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".*

[180] The financial impacts of data breaches, The Information Age, 2018 - https://www.information-age.com/data-breaches-financial-impact-123470254/

[181] IBM Security and Ponemon Institute, 2019 Cost of a Data Breach Study: Global Overview July 2019. Only 2018 and 2017 reports available publicly https://www.ibm.com/downloads/cas/861MNWN2

[182] https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches

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

There are some articles regarding **IoT data breaches**, their prevalence and costs. For example, an article in Information Age[183] notes that staff members could unintentionally cause **enterprise IoT data breaches** as business leaders tend to think about the benefits and under-estimate the risks. For example, in an office environment, there may be breaches internally, such as connected IoT printers being accessible by unauthorised staff or third parties, leading to costly data breaches, which it estimates at about 420,000 EUR[184] per major breach.

The absence of automated updating of IoT software in an enterprise IoT environment was identified as another risk factor that could lead to security breaches by F-Secure in another study. [185] The report notes 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 report also makes the important point that the cause of many of the IoTs problems emanates from manufacturers' supply chains. "Most device vendors license software development kits for the chipsets they use in their smart cameras, smart appliances, and other IoT devices. That's where the vulnerabilities and other issues are coming from," explains Niemela. "Device vendors have to start asking for more in terms of security from these suppliers, and also be prepared to issue updates and patches as they become available." [186]

Cyberattacks leading to breaches of personal data and infringements of privacy may have multifaceted motivations. A significant threat is the use of IoT devices for lateral attacks. "Breaching many IoT devices may pose relatively minor threats in terms of the data held on those devices, but it may provide an entry point for further espionage to access or to compromise sensitive data. As to the **types of internet-connected RE devices that can cause data breaches**, research by Symantec found that **routers** and **connected cameras** make up 90 percent of infected devices. [187]

A report by the Microsoft Security Response Center recently reported it had observed a threat actor targeting a VOIP phone, an office printer, and a video decoder. "The attacker's apparent motivation was to gain access to a variety of corporate networks. "Once the actor had successfully established access to the network, a simple network scan to look for other insecure devices allowed them to discover and move across the network in search of higher-privileged accounts that would grant access to higher-value data". [188]

A study by Digicert [189] found that there are costs for companies of not putting sufficient emphasis on IoT security from the outset. "Companies which place a focus on IoT security early on (top-tier) and are seen as effectively managing IoT have a far lower rate of IoT-related security incidents, with only one-third experiencing a related incident". There were other differences between companies categorised into different groups as to whether they took IoT security seriously or did not give it adequate attention from the outset. Bottom-tier companies were found to be considerably more likely to experience IoT-related security incidents, for example:

- More than six times as likely to have experienced IoT-based Denial of Service attacks
- More than six times as likely to have experienced Unauthorized Access to IoT Devices

[183] https://www.information-age.com/iot-and-data-breaches-123483531/
[184] https://quocirca.com/wp-content/uploads/2019/04/Quocirca_PrintSecurity2019.pdf
[185] https://press.f-secure.com/2019/04/01/iot-threats-same-hacks-new-devices/
[186] Idem.
[187] https://abhijitbhaduri.com/2019/02/25/cybersecurity-should-you-care/
[188] https://www.iotworldtoday.com/2019/08/15/a-year-in-review-12-iot-security-considerations/
[189] Digicert, State of IoT Security 2018 https://www.digicert.com/state-of-iot-security-survey/

- Nearly six times as likely to have experienced IoT-based Data Breaches
- 5 times as likely to have experienced IoT-based Malware or Ransomware attacks

A further finding was that basic measures such as **data encryption and device authentication aren't as widespread as they should be in enterprise and consumer IoT.**

A few examples of major data breaches in the past couple of years experienced by companies are now provided:

- Personal data, including credit card details, passport numbers and the dates of birth of up to 500 million guests, had been stolen in a colossal hack of an International hotel chain.
- A major European airline is facing a record fine of more than £183 million under the GDPR over a customer data breach from the Information Commissioner's Office. Personal data relating to 380,000 passengers was compromised during a hacking incident in 2018.

Some of the challenges in addressing the costs of data breaches and of fraud were underlined In a UK Home Office report[190]**. Cyber breach costs were divided into three categories**: costs in anticipation, as a consequence, and in response. Anticipation costs are preventative measures, such as anti-virus software; consequence costs arise in the wake of a breach, are beyond an organisation's control, and can manifest not only as monetary loss but also in terms of the level of stress and distrust; response costs refer to the costs of criminal justice system agencies responding to a crime.[191]

In attempts to produce overall estimates, the Costs of Cyber Crime Working Group found there are conflicting definitions of cybercrime, differing types of costs, and variation among sectors. Although the Home Office were able to develop an estimate for the cost of cyber-crime to individuals – £1.1bn across an estimated 2,021,330 crimes in 2015/2016 – this estimate does not include any anticipated costs related to responding to cyber-crime (e.g. police and victim services etc.) and this analysis was also not able to estimate the costs of cyber-crime to businesses.[192]

As part of the UK government's National Cyber Security Programme, the **2019 Cyber Security Breaches Survey (CSBS)** was a first step to identifying critical data regarding the impact of cyber breaches and attacks on UK organisations.[193] Organisations overlooked some important factors regarding the full extent of the costs, posing a disincentive to ensuring effective security, and ultimately reducing these costs. Moreover, 'soft' costs, or qualitative metrics, could not be captured by a survey alone as their identification requires more in-depth research. These 'soft' costs can include, for example, reputational damage and the costs of efforts to restore consumer trust through (re)branding and advertising. Another 'soft' cost is the fear of cybercrime.[194] Fear can be detrimental to consumer trust not only in an organisation, but also in digital services more generally.[195] It is important to consider possibly distorted perceptions of online risk, as these shape individuals' behaviours which, in turn, lead to additional implicit costs. For example, a lack of understanding may lead to imprudent use of services without a security guarantee, or a reluctance to submit personal information and data in the first place.

[190] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf

[191] Understanding the costs of cybercrime, the Home Office, UK https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732110/the-economic-and-social-costs-of-crime-horr99.pdf

[192] UK Home Office, The economic and social costs of crime: Second edition, Research Report 99, July 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732110/the-economic-and-social-costs-of-crime-horr99.pdf

[193] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

[194] https://www.techuk.org/images/understanding-costs-of-cyber-crime-horr96.pdf

[195] https://www.mdpi.com/2071-1050/10/4/1015/htm

The earlier cybersecurity breaches are detected leading to personal data loss, the less costly the breach is likely to be. For example, research by the ISACA[196] found that breaches identified within 30 days or less (rather than the average 197 days) saves organisations in the US $1 million in costs.

In relation to the **economic and social costs for consumers** of IoT device breaches, a further study *Quantifying Consumer Costs of Insecure Internet of Things Devices*[197] also provides useful insights, however the focus is on estimating the costs of DDoS and BotNet attacks using IoT devices. The study notes that there is little research to empirically measure costs to the consumers who own the compromised devices used in cybercrimes. *"This lack of research makes it difficult to (1) estimate the total social cost of cyberattacks; (2) determine how costs are distributed among stakeholders; (3) make a determination about which parties are in the least cost avoider position to prevent or mitigate cyberattacks; and (4) protect and compensate consumers and third parties harmed by cyberattacks. Accounting for direct economic losses is important in determining whether consumer protection or computer crime law can be brought to bear on insecurity problems".* Though the costs estimates focus on DoS study, the same study makes useful observations relevant to the present CBA in the IA, such as "*Putting an economic cost on IoT insecurity will inform strategies for regulating IoT devices and enforcing workable security standards to reduce the negative impacts of IoT devices on society".*

Overall, the findings in respect of the costs of data breaches were that:

- There are considerable direct and indirect costs of data breaches for companies;
- There are examples of companies and organisations that have been fined under the GDPR and over time, the costs of regulatory non-compliance ought to have a deterrent effect on non-cybersecure practices relating to the lack of adequate safeguards to ensure adequate data protection and privacy and protection from fraud;
- There are also costs for consumers, including consumer detriment from experiencing a data loss, loss of privacy, data stolen and from fraudulent activities resulting from IoT security breaches;
- Some aspects of the lack of security and / or data breaches in consumer and enterprise IoT are more difficult to quantify, such as the impact of the loss of trust in IoT devices, but nonetheless were found to have a negative impact in terms of market growth.

5.3.12Benefits of activating the delegated acts

Two different types of benefits of going ahead with a regulatory approach by activating the two delegated acts were identified:

1. Benefits on sales volume of enhanced consumer trust in internet-connected RE and wearable RE due to strengthened security (to protect data, privacy and prevent fraud).
2. Impact on value of sales linked to Willingness to Pay (WTP) for strengthened security.

When making purchasing decisions, consumer trust is paramount. Trust in a brand was found to be one of the most frequently mentioned reasons by consumers for purchasing products in a global survey by PWC. [198] Consumers International developed the *Trust by Design Guidelines for consumer IoT,* [199] reflecting the fact that with the growing number of consumer IoT devices in use, consumers are becoming more concerned about their safety and security.

[196] ISACA, Cost of a Data Breach, Time to Detection Saves Real Money - https://cdn2.hubspot.net/hubfs/4039079/Old/ARCHIVE%20%20Nov%2019/013019_Cost%20of%20a%20Data%20Breach.pdf

[197] *Quantifying Consumer Costs of Insecure Internet of Things Devices,* Kim Fong, Kurt Hepler, Rohit Raghavan, Peter Rowland, University of California, Berkeley, School of Information.

[198] Global Consumer Insights Survey 2018 - https://www.pwc.com/gx/en/retail-consumer/assets/consumer-trust-global-consumer-insights-survey.pdf

[199] https://www.consumersinternational.org/media/239715/trust-by-design-guidelines.pdf

The guidelines note that "many consumer IoT (or CIoT) products are coming onto the market with low levels of security or information about how they work or how to use them safely, which could erode trust and participation across this emerging market at a critical stage in its development. Understanding people's reservations and concerns will be important for any manufacturer wanting to produce quality, safe products that meet consumers' expectations and satisfy their concerns. Creating an environment where consumers can be confident that the products they buy meet a basic standard of trust, privacy, security and transparency will benefit everyone involved".

Therefore, as consumer (and broader user) trust is an important element that influences purchasing decisions, the extent to which greater security to protect personal data and privacy and to prevent fraud may lead to increased sales should be considered in the CBA. Previous behavioural science studies into consumer behaviours can help to shed light as to how far, if the two delegated acts were to be activated, this might lead to increased sales (on the basis that consumer trust influences the overall level of consumption).

In order to estimate these benefits, literature has been sought to identify suitable benchmarks for the potential percentage increase in sales if prospective users of internet-connected RE and wearable RE had greater trust in the products through increased confidence in their security to safeguard data protection privacy and to prevent fraud.

The interview programme with manufacturers also found that leading European manufacturers in some product groups for internet-connected RE and wearable RE 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 (e.g. integrating data protection by design and default under the GDPR / Article 25), the primary reason for focusing on security is to embed it within their marketing.

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 cybersecurity, which could help to differentiate it from competitors globally. This was seen as potentially leading to increased sales of internet-connected RE.

If Europe's leading manufacturers in areas such as routers, electrical appliance products, mobile phones etc. perceive that security is an important component of their brand value and reputation, evidently, strengthening consumer trust in the security of internet-connected RE and wearable RE is likely to lead to increased sales.

Some relevant analogous research focuses on consumer trust in online purchasing behaviours via websites. [200] For example, a study was undertaken to analyse how privacy concerns about the internet have had an impact on consumers' intentions to make online purchases. A research model was developed establishing that the impact on consumer behaviour involves a complex interaction between privacy concerns and theories relating to trust and risk, theories about planned behaviours and the technology acceptance model. The study defines technology risks as *"the degree to which individuals believe that if they make online purchases, they will suffer losses caused by the Internet and its technology infrastructure, such as security weaknesses".* [201]

In addition, other research has focused on the extent of trust in purchasing and using consumer IoT devices. [202] It should be noted that consumer IoT devices are often in focus and this type of internet-

[200] Privacy concerns and online purchasing behaviour: Towards an integrated model, Nuno Fortesa, Paulo Rita. https://www.sciencedirect.com/science/article/pii/S2444883416300134

[201] Idem.

[202] 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://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800

connected RE has been in greater focus compared with the wider spectrum of RE. A 2020 study examined the impact of IoT security labelling on consumer product choice and willingness to pay (WTP), the maximum amount that a consumer will pay for a product. The study abstract notes that:

"Security and privacy concerns have been raised about the IoT which impact upon consumer trust and purchasing. Moreover, devices vary considerably in terms of the security they provide. It is difficult for consumers to differentiate between more and less secure devices. One proposal to address this is for devices to carry a security label to help consumers navigate the market and know which devices to trust, and to encourage manufacturers to improve security. Using a discrete choice experiment, we estimate the potential impact of such labels on participant's purchase decision making, along with device functionality and price. With the exception of a label that implied weak security, participants were significantly more likely to select a device that carried a label than one that did not. While they were generally willing to pay the most for premium functionality, for two of the labels tested, they were prepared to pay the same for security and functionality".

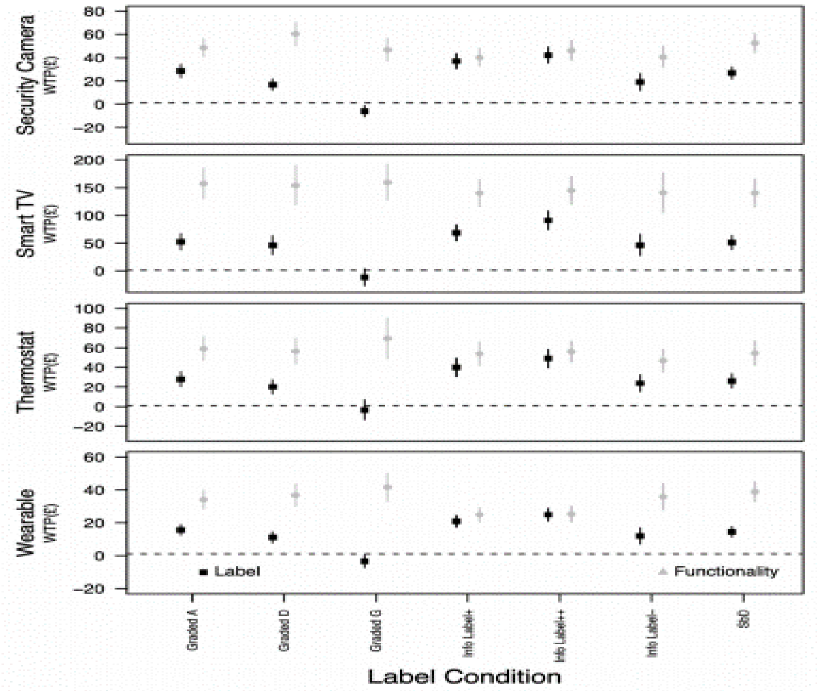
The study addressed the issue as to how much consumers were WTP for the security of IoT devices. The study notes that in an IoT context, *"consumers' mental models of risk and IoT devices may differ as these once everyday objects, such as thermostats and watches, were not conventionally susceptible to online risks. Moreover, research has shown that WTP judgements are context sensitive. As such, consumers may be willing to pay more for certain classes of devices, such as those that are linked to physical security (such as security cameras) or to safety critical services (such as thermostats)".* This finding is highly relevant to the IA study, as whilst analogous, the same principles as apply to IoT security labelling are also applicable as regards security integrated into internet-connected RE.

Consumers are often willing to pay a modest premium for a secure product that protects their data and privacy. As regards the assertion that *"it is difficult for consumers to differentiate between more and less secure devices",* if the delegated acts were to be activated then in the same way that many manufacturers already mention on product packaging for marketing purposes that their products are RoHS and REACH-compliant, firms could make it clear in the packaging that their products are security-compliant with the RED's essential requirements on safeguards to ensure data protection and privacy and protection from fraud.

Participants in the behavioural study which used a discrete choice experiment were willing to pay more for IoT devices that carried a security label. Relative to a device without a label, participants expected to pay between EUR 3.50 and EUR 10.00 less for devices that had a low-security graded label. "*For two of the informational labels, and with the exception of Smart TVs, participants choices suggested that they would be willing to pay approximately the same additional cost for a device that carried a security label as they would for a premium device. In all other cases, participants were willing to pay between 27–63% (mean 40%) of what they were willing to pay for additional functionality".*

An overview of the WTP for different levels of security for an IoT security label is provided (in this case graded on a label from A to G) for consumer IoT products. These products are within the scope of the current study. Although the focus is specifically on security labelling, this data is useful as carrying out a behavioural experiment is a time-intensive and costly exercise which would necessarily be a separate study in its own right.

Figure 5.8: Behavioural experiment – WTP for IoT security labelling for four categories of internet-connected RE



Source: 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. Reproduced with kind permission of the authors.

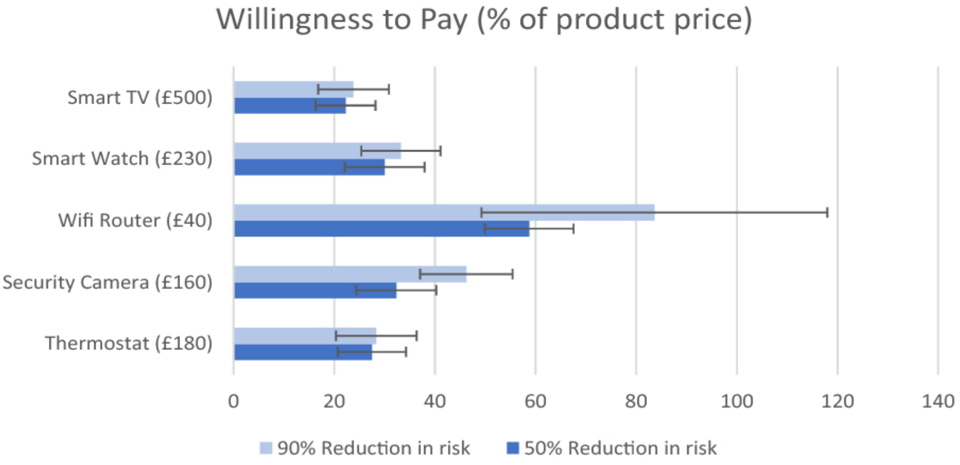
Participants willingness to pay (WTP) for different IoT labelling schemes and functionality. NOTE: vertical bars show the 95% confidence intervals. Source: Pg 14, The impact of IoT security labelling on consumer product choice and willingness to pay - Shane D. Johnson, John M. Blythe, Matthew Manning, Gabriel T. W. Wong

The research found that consumers in the experiment were willing to pay, on average, an additional £48 (SD = 6.5), £148 (SD = 8.0), £34 (SD = 6.0) and £57 (SD = 6.3) for better-functioning security in products such as security cameras, Smart TVs, wearables and thermostats respectively. This is between 29–40% of the average cost of the devices tested willingness to pay (WTP). Our study team's assessment is that this is rather high. A more realistic estimate might be that users of internet-connected RE might be willing to pay 10% to 20% 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 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).

A second paper on willingness to pay [203] was also carried out by the same team of researchers. This showed that consumers were willing to pay significantly more for secure products than they were for non-secure, as shown in the following diagram.

[203] What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Sci 9, 1 (2020), Blythe, J.M., Johnson, S.D. & Manning, M. https://doi.org/10.1186/s40163-019-0110-3

Figure 5.9: Willingness to Pay (% of product price)



Source: What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Sci 9, 1 (2020), Blythe, J.M., Johnson, S.D. & Manning, M (reproduced with kind permission of the authors).

The above percentage estimates are the mean amount that participants reported that they were willing to pay for different types of products and different levels of reduction in risk, both a 90% reduction in risk and a 50% reduction. The cost of each device is shown in (parentheses). The study's results suggest that consumers are willing to pay more for secure IoT devices, but that this is not dependent on the level of risk reduction offered, where a statistically meaningful relationship could not be established to a 95% confidence level. Nonetheless, the study shows that many users would be willing to pay more for their devices.

Research undertaken through the present IA study also found that many manufacturers believe that investing in product security can potentially **deliver increased sales, but also to enhance their brand value and tacitly it is seen as a *de facto* requirement.** If consumers are willing to pay a slight premium for such products, then there would not only be higher sales volume, but these would be worth greater value. Whilst this is difficult to quantify, qualitative feedback from the product case studies suggests that consumer preferences in Europe are trending towards purchasing more secure products. For example, one of the manufacturers interviewed for the routers case study noted that whereas five year ago, there were very cheap home routers on the market, their market share has been reduced as consumers prefer to purchase medium-cost routers in the €50-100 price bracket rather than the cheapest available unbranded and/ or less recognised brand products (€30 EUR).

An estimate of the benefits from enhancing consumer trust under a base case scenario is provided below. When developing the quantitative hypothesis, relevant literature was considered, such as those mentioned in footnotes, and qualitative feedback from the interview programme and from the product case studies.

Table 5.11: Estimated benefits from enhanced consumer trust and WTP consumer preferences

Product type	Impact on sales volume of products sold (%)	WTP for more secure products - % increase compared with baseline (%)
All internet-connected RE and wearables	5%	5-10%
Routers	5%	10-15%
Laptops	5%	10-15%
Baby monitors	10%	10-15%
Security cameras	10%	10-15%
Smart domestic appliances	10%	5-10%

Product type	Impact on sales volume of products sold (%)	WTP for more secure products - % increase compared with baseline (%)
Robotic lawnmowers	5%	2%
Smart thermostat	5%	2%

Some internet-connected RE involves purchases that users often have to make, for example for home and business use, such as a router, mobile phone and a laptop. Therefore, the sales volume from producing more secure products is unlikely to increase that much, although the product group might benefit marginally from increased consumer trust. Conversely, other RE and wearables may involve discretionary purchases and therefore, there is a greater potential demand-side elasticity if the product is made more secure to protect personal data and privacy (e.g. baby monitors, smart domestic appliances). In the case of domestic appliances, for example, consumers also have a choice as regards whether they buy a conventional fridge, thermostat, oven or washing machine, or a smart internet-connected appliance that contains RE. Therefore, for such products, strengthening security could have a much more significant impact on demand by accelerating technological adoption.

Conversely, for the same categories of RE, WTP for more secure products could be higher among users purchasing internet-connected RE that they are obliged to purchase anyway, as frequent users of such RE may place a value on additional security features, not only product performance and functionality. Some manufacturers stressed that their customer base expects security along with high-performing functionality and these product features cannot easily be separated.

In the case of robotic lawnmowers, the underlying rationale for the lower estimate for WTP is that the case study research found that such products submit very limited personal data back to the manufacturer, such as the IP address, other than during product registration. Conversely, consumer trust has a general positive effect across all internet-connected RE products.

5.3.13 Summary findings - the quantification of costs

This section sets out the overall findings from the quantification of costs and working assumptions underpinning the Cost Benefit Analysis (CBA). These draw on the data collected through the interview programme and targeted online consultations, as well as the detailed review of secondary literature.

This section firstly addresses administrative costs. Subsequently, it presents cost estimates related to data breaches, and concludes with the findings in respect of the substantive compliance costs and the potential costs that would be incurred by market surveillance authorities.

5.3.13.1 Administrative costs

As explained earlier in the typology of costs, the main types of administrative costs analysed were:

- Testing costs (internal, external);
- Familiarisation with the essential requirements pertaining to Article 3(3) (e) and (f) prior to placing products on the market;
- Preparation of technical documentation (e.g. updating the Declaration of Conformity (DoC), preparing and / or updating a technical file to reflect any technical standards used to comply with the activation of Art. 3(3) (e) and / or 3(3) (f)); and
- Checking compliance with other EU legislation – including whether any previous testing results - could be used to help demonstrate compliance with Art. 3(3) (e) and / or 3(3) (f).

5.3.13.2 Testing costs:

Third-party testing was identified as being the costliest type of administrative cost, as three-quarters of respondents to the targeted survey agreed that third-party testing costs may be either high or somewhat high should the DAs be activated, with the remainder deeming these costs to be either moderate or low.

However, a crucial issue raised was the difficulty for many economic operators and industry associations in ascertaining the level of testing costs, as the delegated acts are as yet not elaborated in terms of their detailed implementation.

It was therefore seen as insufficiently clear at this stage whether testing carried out under other EU legislation (e.g. GDPR Art. 25 or by manufacturers voluntarily participating in the CSA) would be sufficient to avoid retesting under the RED. Some stakeholders found it difficult to assess the level of costs. Nonetheless, some third-party cost estimates are provided below:

The costs of testing will vary depending on a number of factors such as the volume at which the manufacturer produces, the complexity of the product itself, and whether testing is carried out internally, by a third-party or involves both.

- The **perceived potential high costs of third-party testing under Art. 3(3)(e) and Art. 3(3)(f) were** seen as a concern among some stakeholders (especially industry associations and manufacturers). However, the costs of testing incurred by large firms/multinationals producing internet-connected RE may be characterised by high BaU costs, as most such firms already integrate security functionality into the design, engineering and manufacturing of their products.
- **Simple internet-connected RE:** Manufacturers estimated that the testing costs for such RE ranges between €5,000 - €10,000 to carry out basic cyber-security checks (between 2 and 5 days). €7,500 (the median value within this range) was assumed to be the "typical cost of testing" for this product type. This means that total testing costs for simpler RE products is around €3,600-€4,800.
- **Complex products**: A representative from a testing body estimated that the costs of testing are around €1,200 per day, with differences between simple and complex products in the time required to test products. A minimum of 2-3 weeks and a maximum of several months is required for more complex products (e.g. smartphone). The typical testing costs for complex products were in the order of €20,000 - €30,000, but the cost range varies widely, depending for instance on complex the RE is, how software-intensive etc.
  - Testing a more specialist, niche product was estimated by an interviewee from a testing lab to cost between 30,000 EUR and 40,000 EUR. 35,000 EUR (the median value within this range) will thus be assumed to be the "typical cost of testing" for this product type.
  - Internal and external testing costs can be as high as €150,000 in the case of the costs for major manufacturers in testing for security ahead of a product launch.
- **Certification costs**: A representative from a certification body estimated the costs of certifying simpler RE products covered under the RED at €2,000 – 5,000, as compared with €10,000 – 20,000 for more complex RE products.
- As SMEs often do not have their own in-house testing capabilities, unlike large firms and multinationals, **SMEs perceived that the testing costs could be proportionately higher in per unit terms.** To understand the costs of testing incurred by European SMEs producing high-volume RE simple products, 7,500 EUR was multiplied by the total number of SMEs manufacturing these types of products. A testing body highlighted that it may be financially prohibitive for SMEs to invest in more than five-days of testing, which implies a maximum ceiling of 10,000 EUR for simple products.
- However, the costs of testing more complex internet-connected RE for security safeguards for

data protection and privacy and protection from fraud may be prohibitive for SMEs if the products concerned are produced in low volume. This would be less of an issue if the SME expects to sell in higher volume, since as with large firms, the overall compliance costs could be mitigated by manufacturers across a high volume of products to spread the costs per unit. For example, the cost per unit of strengthening router security was estimated to be circa €0.355 in terms of testing costs, but this would depend on which technical requirements are incorporated in future technical standards. Some technical solutions are low-cost (e.g. absence of default user names and passwords) whereas others are higher-cost (e.g. encryption, but even for the latter, the evidence base on additional costs is somewhat nuanced).

- The total estimated range of external testing costs incurred by SMEs producing complex internet-connected RE products and devices is in the order of €15,000-€35,000 (median €25,000). However, how costly this is depends on the volume of production. Other administrative costs

Other administrative costs incurred by manufacturers are now considered.

The first step in the compliance process would involve **familiarisation with the essential requirements.** The explanation in the legal text of the RED itself only consists of a single line each for Art. 3(3)(e) and 3(3)(f) respectively. This would take minimal time for manufacturers to digest. However, there would need to be human resource investment by product engineers and legal compliance staff to familiarise with how the activation of these articles and any obligations differ with those under the GDPR's Art. 24 and Art. 25. They would also need to familiarise with harmonised technical standards and to review which could serve best to demonstrate compliance with the essential requirements.

On average, the interview feedback suggests that familiarisation would take two FTE a period of one month. On the assumption that the average salary for staff involved (engineers, managers) is c.a. €55,000, this implies a cost of circa €9,200 in staff costs. These would be mainly one-off costs, however, some recurring costs might be incurred linked to new product launches.

Regarding the **preparation of technical documentation**, this will firstly involve **updating the Declaration of Conformity (DoC),** and secondly **preparing and / or updating a technical file** to reflect any technical standards to comply with the activation of Art. 3(3)(e) and / or 3(3)(f)). Updating the DoC was seen as a simple task, which would incur minimal costs. However, updating technical documentation to ensure that minimum baseline security requirements were complied with at the product level would require time input. It is estimated that this would take on average circa two FTE months. Using the same salary costs benchmark, this implies a cost of circa €18,400 in staff costs.

5.3.13.3 The costs of data breaches

There are high costs of data breaches. The average total global costs of a data breach are 3.92 million USD, although average costs were significantly lower in Europe than the US. Below estimates related to the costs of data breaches and cyber-attacks directed towards internet-connected RE devices and products are provided, considering how these costs could be mitigated by activating the delegated acts possible under Art. 3(3)(e) and 3(3)(f) of the RED.

- 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 a response 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 USD. 204 However, estimates as to the costs of IoT attacks and of data breaches vary considerably. For instance, a Cyber Security Breaches Survey found

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

that the average cost of a cyber breach or attack against an organisation in the UK was £4,180 in 2019, rising from £2,450 in 2017.

- For example, according to an *Annual Survey on the Costs of a Data Breach* [205] , the costs of a data breach (including follow-up remedial action, compensation for data losses are $3.92 million on average globally, though the costs in the US are typically a lot higher than those in Europe. 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.
- There are also costs associated with the detriment experienced by users of internet-connected RE due to a loss of data protection and privacy. Non-sharing of data subsequently by data subjects has an economic cost, as in the context of a big data society, data has a value, and therefore, greater reluctance among consumers and professional users of such RE would carry costs.
- In addition, there are also direct losses from data breaches due to fraud. The UK's Home Office estimated that cyber-crime in the UK cost £1.1bn to individuals. This does not include any costs related to responding to cyber-crime (e.g. police and victim services etc.). The analysis was not able to estimate the costs of cyber-crime to businesses. It may be assumed that the activation of the RED DAs could significantly reduce direct financial losses, as well as reduce the level of detriment.
- In instances when manufacturers of internet-connected RE are already implementing security by design and default principles, the assumption is that there are cost-savings associated with protecting different types of devices and products with security vulnerabilities that are more commonly targeted by hackers through avoidance of the costs of data breaches.
- According to a study[206], manufacturers of cameras and routers who do not presently 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 manufacturers would therefore incur new compliance costs upon the activation of DAs, whereas for the other half, estimating the costs could involve making a discount to reflect the BaU costs (estimated at 70-80%), as some manufacturers are already following good practices in these areas.
- However, manufacturers investing in strengthening the security of internet-connected RE would benefit from cost savings of circa €100,000 on average due to avoiding the high costs of data breaches for manufacturers and other economic operators. As noted earlier, these costs were found to stem from:
  - Direct costs relating to the data breach itself – e.g. informing customers about the breach, taking direct action to plug the breach.
  - Remedial action to address and prevent future breaches.
  - Indirect benefits (i.e. avoidance of potential high costs of reputational damage).

Although costs related to reputational damage are difficult to estimate, **firms can lose up to 40% of their customers following data breaches.** According to a PCI Pal survey, 44% of customers in the UK claim they would stop spending with a business for several months following a data breach, while 41% declared they will never return to a business post-data breach.

According to a survey of 700 firms, only 49% of companies make security a part of their product design lifecycle process. It can therefore be assumed that the activation of the RED DAs and addressing

[205] IBM/ Pokemon Institute, Annual Survey on the Costs of a Data Breach

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

security vulnerabilities upfront could save approximately 50% of manufacturers of internet-connected RE that are not already investing in security the potential economic damage and disbenefits of a costly data breach (of up to €100,000). It can therefore be argued that the high costs of a data breach means that investment in baseline security requirements upfront through adherence to security by design and default principles would pay for itself (under Options 2, 3 and 4). These benefits could also materialise under Option 0 (status quo option) and Option 1 (voluntary approach) but only if voluntary measures were taken by manufacturers of internet-connected RE to implement baseline security requirements.

5.3.13.4 Substantive compliance costs

78% of the economic operators who took part in the targeted consultations thought that some substantive compliance costs would materialise. The majority of these stakeholders perceived that substantive costs would mainly consist of research and development-related costs, due to a need to redesign chipsets or components and to design new compliant products.

Several large and globally-reputable manufacturers interviewed considered substantive compliance costs to be largely BaU costs, as many manufacturers are already implementing security by design and default principles and complying with GDPR obligations regarding data protection by design and default from the outset. An increasing number of manufacturers are taking data protection and privacy principles into consideration at each and every stage of product development. Whilst this suggests high BaU, this is very difficult to quantify.

However, other manufacturers were concerned about the costs, as the DAs have not yet been defined in detail, nor the technical requirements as regards baseline security requirements that would underpin them. It is therefore unknown how far any new requirements would diverge from, or go beyond existing requirements under the GDPR.

Substantive costs were found to be very difficult to quantify until more detail has been worked up on this legislative initiative. However, qualitative research points to evidence of a **positive overall cost-benefit relationship from manufacturers making investment in strengthening the security of internet-connected RE**. A benefit of investing in security is avoiding the additional substantive compliance costs of not taking action to address security issues through the implementation of security by design and default from the outset. It is axiomatic that addressing problems post-market placement is more costly than addressing them at the design stage. Although somewhat dated (2009), a number of quotations obtained [207] supported this view:

- If only 50% of software vulnerabilities were removed prior to production, costs would be reduced by 75%. *Source - Gartner.*
- Correction of security flaws at the requirement level is up to 100 times less the cost of correction of security flaws in fielded software - *Source - Fortify.*

Interviewees in the current study also pointed to security by design and default being a cost-effective approach.

Activating the two DAs should be cost-effective provided that coherence is ensured with other legal requirements, especially those relating to data protection and privacy where there is already some legislation in place, and therefore compliance processes (and costs incurred) in addressing one piece of legislation could help to demonstrate compliance with the RED DAs.

[207] See How to Create a Business Case for Software Security Initiatives by Marco Morana OWASP Lead TISO Citigroup (https://www.owasp.org/images/7/7b/OWASP-Italy_Day_IV_Morana.pdf)

6. Conclusions

6.1 Conclusions and recommendations

In this section, the conclusions and recommendations from the impact assessment study are outlined. Problem definition

6.1.1 Penetration of connected RE devices in European households

- As digitalisation has become a major driver of European industrial competitiveness, there is a rapidly growing number of internet-connected radio equipment (RE) devices and wearables on the European market, both consumer and enterprise products[208] .
- This trend is expected to increase further in future, with estimates of up to 20.4 billion units of such devices globally by 2020 (Gartner), of which an estimated 7.43 billion in the European Union by 2030 (Tech4i2).
- Market demand forecasts predict that cumulative annual growth of 14.6% for internet-connected radio equipment devices and wearables will be achieved between 2015 and 2030, which equates to more than 28 RE devices in each EU28 household by 2030 (excluding RFID and medical devices).
- The marked growth in demand for such devices has been driven by a number of big picture trends, such as the transition from the internet to the Internet of Things (“the IoT”), in which devices and sensors are interconnected, many of which are capable of transmitting data in real-time back to the manufacturer, technology or service provider, and some of which share data with other connected devices (e.g. in a home or enterprise network).

6.1.2 Security vulnerabilities in connected RE products and wearables

- In parallel with the increased number of such devices and wearables on the market, there is growing recognition that many such internet-connected radio equipment devices have security vulnerabilities.
- These range from simple flaws, such as a lack of in-built basic security features, using default usernames and passwords, a lack of encryption and authentication requirements and the absence of two-step security verification through to more sophisticated cyber threats, such as malware, TCP injections, phishing, and ransomware attacks with perpetrators seeking payment in cryptocurrency. Furthermore, at present, many such devices currently lack the resources (e.g. processing power etc.) to implement certain security mechanisms.
- Many of the risks however are common across multiple different types of internet-connected radio equipment and wearables, and therefore, the security vulnerabilities are less associated with specific devices and more with the fact of being connected directly to the internet.
- There are also risks linked to indirectly internet-connected radio equipment and wearables, but these are of a lower degree of magnitude than for devices that are directly connected.
- Security vulnerabilities were found to be especially acute in consumer IoT devices, as such devices often have a lower level of security and encryption compared with enterprise-grade devices (e.g. see case studies on routers, laptops).
- Nevertheless, in an enterprise IoT environment, vulnerabilities in insecure systems are being sought by hackers and by automated bots to steal sensitive data and/or install harmful malware.

[208] There is a blurring between the consumer and enterprise market segments that would make it difficult to have a differentiated regulatory approach between consumer products and products intended for professional users, as many products are used by both.

- Further to this, a number of stakeholders highlighted software vulnerabilities, namely the severity of risks if/when consumers do not update their devices' software or if/when manufacturers stop sending security updates. Although this is outside the study scope, software is inextricably linked to internet-connected RE devices, adding another layer of vulnerabilities.
- Whilst recognising that the IoT has considerable socio-economic potential, the vulnerabilities identified in many IoT devices means that there is a risk of device-level data breaches which could potentially lead to data protection and privacy, and protection from fraud being compromised, with considerable costs for manufacturers, enterprises and consumers.
- Growing awareness about security vulnerabilities and the threats of individual device and network-level penetration has prompted national governments, industry and consumer associations to develop good practice guidance on data protection by design and default (under the GDPR) and the broader principle of security by design and default (which has the potential to stop data breaches from the outset).
- Additionally, there are many examples of good practices being adopted by individual manufacturers to ensure that security, data protection and privacy and protection from fraud are integrated into the design phase from the outset (i.e. 'security by design').
- However, equally, the literature, interviews and results from the targeted and OPC consultations point to many examples of bad practice in the design of internet-connected RE products and wearables, with some devices and products having not even the most basic security functionality, thereby rendering data at risk of theft.
- Moreover, where non-secure internet-connected RE products and wearables have been identified by market surveillance authorities, these remain on the European market, even if they are insufficiently secure to ensure that consumers and businesses have their personal data and privacy protected, with a clear risk of financial, identify and other types of fraud.
- Responsibility is often placed on the consumer to ensure that their connected RE products and devices are secure. However, consumers often lack understanding of product and device security and how their data protection and privacy might be compromised through connected RE products.
- Stakeholders (targeted survey and interviews) recognised the risks associated with security vulnerabilities in internet-connected RE products, especially for vulnerable users, namely children and the elderly.
- The study found that there are commonalities across many internet-connected RE products and devices in terms of the types of security vulnerabilities. Many of these stem from being directly connected to the internet, and therefore at risk of hacking, rather than to the characteristics of the device itself.
- In terms of the magnitude of risks, whereas directly internet-connected RE poses a higher level of risk, RE products that are indirectly internet-connected (via radio wave communications technologies such as Bluetooth) still pose some lower level risks as the device would have to be penetrated by a localised threat in geographic proximity (e.g. ranging from 10m to 50m usually, although in some cases up to 250m away. A problem in the context of the growth of consumer and enterprise use of IoT devices is that the risks associated with individual devices are compounded by network-related risks. Whilst the latter are outside the formal scope of the RED, they present an entry point to vulnerable IoT devices within home and enterprise networks.
- The increased frequency of cyberattacks at device and network level, and the growing sophistication and complexity of such attacks, makes them more difficult to detect. This affects both enterprise and consumer IoT devices, but is a particular problem among internet -connected RE products and wearables, especially consumer IoT, which may lack any basic security, and also lack encryption and authentication functionalities.

6.1.3 Extent of protection in existing EU legislation and analysis of regulatory gaps

- The challenges associated with maintaining the security of IoT products are being examined by a number of regulators globally, such as at EU level through the present study, the U.S., where California has adopted regulation stipulating baseline security requirements in consumer IoT devices (with federal level regulation also being actively considered). In the U.K, an industry code of practice was developed in 2018, but following a May-June 2019 consultation, consideration is being given as to whether a regulatory approach would be more effective, possibly building on some of the principles outlined in the ETSI standard on consumer IoT.
- The EU legal framework regarding data protection and privacy was considerably strengthened through the entry into force of the GDPR in May 2018, and the privacy of personal communications data has been required by law since the e-Privacy Directive was adopted in 2002.
- The alignment of the proposed e-Privacy Regulation with the GDPR was found to be a positive step forward that would afford users of internet-connected RE products and devices greater protection of electronic communications data submitted online. A wide body of literature has been examined through the study specifically examining how the GDPR is implemented in an IoT context. There remains uncertainty as to how effective the GDPR has been in changing business practices and in protecting users' personal data and privacy, in particular, Art. 25 data protection by design and default and Art. 24, requiring organisational and technical measures to be put in place.
- As the GDPR only came into effect in May 2018, whilst there have been fines issued, there have only been three legal cases on Art. 25 GDPR and one on Art. 35 (Data Protection Impact Assessments where higher risks are identified). Therefore, the absence of more comprehensive data about legal cases and fines (and no cases yet involving manufacturers of RE devices, evaluation materials on what impact the GDPR has had is a limiting factor in the analysis.
- Furthermore, the extent to which existing EU legislation leaves regulatory gaps regarding internet-connected RE devices and wearables has been examined. A key finding is that the GDPR and proposed e-Privacy Regulation could, if implemented effectively and adequately monitored and enforced vis-à-vis the most relevant Articles to the IoT, strengthen the protection of personal data and privacy in such devices and wearables.
- Notwithstanding, there remain regulatory gaps in current EU legislation, which may require more technical interpretation of GDPR for instance by further specifying the rules relating to data protection and privacy and protection from fraud more explicitly into the RED.
- The GDPR sets out data protection and privacy rules relevant to the IoT, such as the importance of obtaining unambiguous consent, but the requirements are directly applicable to data controllers. Manufacturers and other economic operators in the value chain such as technology and service providers could be more explicitly brought within the scope of the delegated acts than they are in the GDPR, where they are referenced in the recitals, but the focus is on whichever economic operator or organisation is the data controller.
- Moreover, there is evidence of low compliance with Art. 25 of the GDPR in the area of internet-connected RE devices and wearables. Many products continue to use default user names and passwords, which suggest that Art. 25 is not being treated as seriously as it should be.
- Although more information is needed through studies and evaluations of the GDPR, our research pointed to some manufacturers not fully complying with the existing rules. This was partly due to difficulties in interpreting how certain aspects of the GDPR might be translated into operational business practices, especially in an IoT context in which artificial intelligence is often used to gather, analyse and act on data, for example, to deliver more user-focused content and for the purposes of targeted advertising.

- Some manufacturers pointed out that whilst the majority of manufacturers are compliant, some market participants at the cheaper end of the market may not be compliant with the essential requirements in the RED, or the requirements on data protection by design and default under the GDPR. As such products are sometimes placed on the European market for a short period and then replaced by other new products (i.e. some products have a short lifecycle), irrespective of whether the delegated acts in the RED were to be activated, such manufacturers would continue to be non-compliant, creating an uneven playing field. Balanced against this was the argument put forward by other manufacturers that many European consumers purchase reasonable quality products, and connected RE products at the very cheapest end of the market are less frequently purchased than was the case 5-10 years ago due to their low quality (e.g. routers, where telco network operators are the main purchasers and they want to ensure that products provided to their customer base offer reliable performance and security features in-built.
- This is perhaps surprising, given the scope for fines to be issued if data protection and privacy is not integrated into products by design and default from the outset. However, it is possible that the situation will improve in the near future (1-3 years), as manufacturers become more familiar with the GDPR's requirements and as more case law becomes available to incentivise manufacturers to take these issues more seriously in product design, and in R&D&I processes.
- A further gap relates to the lack of enforcement powers for MSAs to remove non-secure products from the market that may compromise personal data protection and privacy (which would make them non-GDPR compliant). For example, if consumer IoT devices lack basic security features, such products cannot presently be removed from the market even if they are identified as posing risks to the security and safety of consumers, as the relevant delegated acts in Articles 3(3)(e) and 3(3)(f) have not yet been activated.
- Whilst the GDPR provides some legal protection, it does not allow scope to remove non-compliant internet-connected RE products from the European market. Consequently, some Member States have had to rely on a range of national legislation to withdraw products from the market that were non-compliant in terms of basic security functionality and which risked compromising data protection and privacy (e.g. the Cayla doll). The emergence of a patchwork of national legislation in the absence of clear EU-level legislation also risks undermining the Single Market.
- Whilst the non-activation of the delegated acts in study scope restricts MSAs by preventing them from removing products from the market under the RED, it should be recalled that under the GDPR, fines may be issued of up to 20 million EUR (or a maximum of 4% of global turnover). Moreover, the proposed administrative sanctions under the proposed future e-Privacy Regulation will be aligned with the GDPR.
- Economic operators therefore already have a strong financial incentive to avoid non-compliance with EU rules on data protection and privacy. In terms of regulatory gaps in the RED, presently, the essential requirements focus on product safety but not on security, which is regarded by some stakeholders as a gap. This means that manufacturers are not explicitly required in the Directive to implement measures to ensure data protection and privacy safeguards, but rather to follow other applicable legislation e.g. the GDPR and the e-PD.
- There are presently no explicit references in the RED's essential requirements to product and device security. However, the 2014 Directive does make provision for the potential activation of such requirements through delegated acts (Art. 3 (3)(e) and Art. 3 (3)(f), which could strengthen GDPR implementation by providing technical solutions relating to minimum security baseline requirements to help translate the obligations under the GDPR into requirements relevant to internet-connected RE products and devices in an IoT context.
- The importance of recognising the close link between designing a safe and a secure product was noted by many stakeholders taking part in the consultations. Stakeholders pointed out that

adhering to security by design and default principles (and integrating these into business processes) is a pre-requisite if manufacturers and product designers are to be GDPR-compliant with Art. 25 GDPR requirements relating to data protection by design and default.

- In an IoT context, there were found to be some challenges in terms of how the GDPR requirements are translated into business processes and practices by manufacturers and third-party service providers to ensure data protection and privacy in internet-connected RE products and wearables. A possible solution is that minimum baseline security requirements could be introduced, as is being considered in other regulatory jurisdictions globally, as without adequate security to prevent data breaches, such products cannot ensure data protection and privacy, or protection from fraud.
- There is also the challenge of striking a balance between the possibility of large amounts of data collection that RE-connected devices and wearables may offer on the one hand, and the need to respect the data minimisation principle and proportionality highlighted in the GDPR on the other. This is an example of the challenges in implementing the GDPR in an IoT context in respect of smart RE products.
- In terms of protecting users of internet-connected RE products and devices against fraud, there was found to be a general absence of any relevant EU legislation, outside of the legal text of the RED, which makes provision for the possible activation of a delegated act through Article 3(3)(f)). A challenge in implementing the delegated act is that whilst the text refers to ensuring 'safeguards to ensure protection from fraud', a definition of fraud in the context of connected RE products and wearables would need to be provided. However, this could be provided in the delegated act itself. The definition should be clear but sufficiently broad to reflect the reality that fraud in an IoT context is constantly evolving and should not be confined to financial fraud and identify theft alone, but could be defined as including other types of fraud possible as a result of personal data breaches, such as ransomware attacks, cryptojacking, the cloning of RFID/ NFC cards and formjacking.
- Several stakeholders expressed the view that whilst a clear definition is needed, this should remain broad, due to the evolving nature of frauds perpetuated via internet-connected RE products, both consumer and enterprise IoT devices. This was due to the evolving nature of threats and vulnerabilities across different types of such products

6.1.4 The collection of personal data from connected RE products and wearables and privacy implications

- The transition from the internet to the more dynamic environment of the Internet of Things (IoT) in which devices, objects (especially sensors) are internet-connected, gather large amounts of data and may transmit data to other devices poses challenges from a device security perspective, as well as in relation to data collection and privacy and protection from fraud.
- The potential for data misuse stems not only from technical security vulnerabilities that may result in data breaches, but also manufacturers and service providers collecting data where the consumer may not be clear that their data is being collected and usage of the IoT product being monitored in real-time, as well as processing of personal data beyond the stated purpose.
- The GDPR has strengthened regulatory protection for individuals' personal data and privacy by providing a regulatory framework in which data collection and processing takes place. For example, the requirement under the GDPR for unambiguous consent to collect and process data and on proportionality in data collection (data minimisation) provides protection for users of such RE devices and wearables. However, many consumers remain unaware about i) what data is being collected, ii) for what purpose and iii) how this might be utilised in a big data context by manufacturers, technology and service providers.

- The growth in the use of machine learning and AI in connection with the IoT means that some internet-connected RE products and devices collect data on either an autonomous, or at least semi-autonomous basis, which also raises issues around the need for users to be able to more easily review and update their consent in real-time. There are challenges in integrating user interfaces into some types of RE devices and products, which prevents users from reviewing and updating their consent and changing the privacy settings as easily as they should be able to.
- Balanced against this, the use of machine learning and AI technologies to collect big data also has legitimate business purposes and could bring significant further economic benefits for manufacturers of internet-connected RE products and devices and other economic operators in the value chain. Therefore, if the delegated acts were to be activated, as with the GDPR, a balance needs to be struck between ensuring that rules relating to data privacy and protection are complied with, but without introducing additional stricter rules that could damage innovation and competitiveness in emerging industries linked to data analytics.
- As the RED's scope relates to the period up until placement on the market, it was recognised that some principles relate to ensuring a lifecycle approach to product security, such as regular software and firmware updates and ensuring that service providers maintain data protection, privacy and anonymity in the collection of data from internet-connected RE products and devices by manufacturers post-placement on the market. Some stakeholders suggested that this could potentially be ensured by activating several delegated acts in parallel, i.e. Art. 3(3)(d), 3(3)(e), 3(3)(f) and 3(3)(i) and 4(1). Otherwise, the lack of software and firmware updates could make particular devices more vulnerable, which could then expose other such internet-connected RE devices to device penetration.
- Overall, irrespective as to which policy option the Commission determines is most appropriate to address the problem (see section 6.1.3), a holistic approach to addressing the problems identified in the baseline assessment will be needed. It will be important to take into account the complex nature of global value chains (GVCs) to strengthen data protection and privacy and protection from fraud.
  - Complex products are not inherently riskier in terms of penetration of the device itself compared with simple products in that all internet-connected devices can be penetrated via a hack. However, the fact that they collect extensive personal data compared with simple products means that there are more frequent problems as there are many different pieces of software and apps via which the device might be penetrated voluntarily downloaded on the users' device (e.g. laptops, mobile phones).
  - Moreover, there are more complex GVCs – including outside the EU – associated with complex products, as there are likely to be a series of actors in the value chain responsible as data processors with the data controller responsible for managing this complexity under the GDPR. The more complex the value chain, the more difficult it may be for the manufacturer to check security vulnerabilities directly.
  - However, examples of good practices were identified that show that leading global manufacturers make their supplier base along GVCs responsible for ensuring compliance with all relevant EU legislation (including GDPR and the e-PD).

It has also been found that manufacturers of complex products typically have longer experience and maturity in terms of managing product security (e.g. laptops, smart phones) than manufacturers of IoT products that have only recently been brought to the market. As such, a correlation between the complexity of products and increased cybersecurity risk does not appear to exist.

6.1.5 Analysis of stakeholder consultation feedback

Extensive consultations have been carried out through this IA study and an assessment of stakeholder feedback was produced.

A major interview programme has been undertaken with 76 stakeholders, representing industry, consumer associations, national authorities and market surveillance and enforcement authorities (see Annex 3 for an overview). The results from the targeted stakeholder consultation and the Open Public Consultation (OPC) are presented as standalone documents in Annexes 6 and 7 respectively. The overall findings are now summarised:

- The stakeholder consultations found there to be a broad consensus among stakeholders that many internet-connected RE products and wearables products and devices 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 RE products and wearables.
- 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 RE products, as the nature of security vulnerabilities and threats, especially in relation to fraud, evolve rapidly.
- Stakeholders recognised that if the DAs were to be activated, it would be quite difficult to make the essential requirements only applicable to directly internet-connected RE products using a Wi-Fi connection, as Bluetooth and other similar communications protocols allow for wireless data sharing and are connected to the internet, albeit indirectly. Although simple Bluetooth devices are arguably lower risk as to be penetrated a user would need to be in close proximity, it would be difficult to regulate only Wi-Fi products, but not products with Bluetooth capabilities as many RE products include both Wi-Fi and local connectivity 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 Cybersecurity Act (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 RE products, 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, that it could not be guaranteed that internet-connected RE products 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.

Stakeholder feedback has also been integrated into the analysis of policy options, costs, benefits and impacts provided in the next sub-section.

6.1.6 **Analysis of policy options, impacts and CBA:**

The research has assessed a number of the different policy options defined in the Tender Specifications. Feedback on these options was gathered through desk research (e.g. the findings from the Commission's inception impact assessment in January – March 2019), complemented by an analysis of interview feedback on the options gathered through the targeted and OPC consultations.

6.1.6.1 Option 0 - Relying on existing EU legislation to achieve policy objectives

- The first option – **baseline scenario of relying on existing EU legislation** –viable at least in respect of data protection and privacy, as the GDPR and the proposed e-Privacy Regulation (which will align the current e-Privacy Directive with the GDPR) ensure that data controllers take responsibility across the value chain for ensuring data protection and privacy.
- However, although existing legislation sets out important rules such as the importance of obtaining user consent before data can be collected and processed, it also leaves a number of regulatory gaps.
  - The GDPR is addressed at data controllers, and not explicitly at manufacturers or technology providers. An argument was made by some stakeholders that this could be rendered clearer in the RED by specifying particular data protection rules that are applicable to all economic operators in the value chain.
  - As the GDPR only came into effect in May 2018, there is a lack of evaluation materials as to its implementation and enforcement at this early stage, especially in the context of how GDPR rules are being implemented in an IoT environment. Available literature suggests that GDPR implementation in the fields of information security and industrial products is an emerging area, where there are some grey areas as to how the law should be implemented in practice.
  - There is a perception among some stakeholders that the legislation is insufficiently tailored to address data protection and privacy issues relating to connected RE products and devices, or industrial products more broadly.
  - There is a tension in the GDPR between the stress on the proportionality of data collection (data minimisation) and big data analytics-driven business models, such as those examined through the product case studies (e.g. see Smart TVs). Whilst this is not specific to IoT - and must be resolved within the GDPR, it is nevertheless an important issue as it is especially relevant in an IoT product context, and therefore affects internet-connected RE falling under the RED' scope.
- Under the GDPR (and in future under the e-Privacy Regulation which will be aligned with GDPR sanctions), whilst significant fines can be issued which could have a deterrent effect as regards manufacturers taking short-cuts, under the RED, there is no legal means of removing non-secure connected RE products and wearables that do not provide adequate device-level data protection and privacy and/ or protection from fraud from the European market.

- The CSA remains voluntary, and therefore does not provide any regulatory protection for users of internet-connected RE products. It is also too early to assess either the CSA's impacts, in terms of whether it will have a positive impact on manufacturer behaviour by pushing further consideration of security by design and default principles from the outset, as a means of being GDPR compliant in respect of data protection by design and default.
- Overall, this option would only be viable in addressing concerns regarding security vulnerabilities in connected RE products which risk compromising data protection and privacy if there were to be a greater focus on strengthening the enforcement of GDPR towards the relevant actors. In particular:
  - Greater attention could be given by Data Protection Authorities to raising awareness of Art. 25 GDPR among manufacturers and checking compliance.
  - Greater use could also be made of Data Protection Impact Assessments (Art. 35) by manufacturers wherever there is uncertainty as to whether particular business practices relating to data collection and processing from smart products raises specific issues.
- The assessment of relying on existing legislation was restricted to some degree by the absence of an evaluation of the GDPR, or of its impact on manufacturers of internet-connected RE products and devices.
- Relying on existing EU legislation would not be feasible in the case of ensuring safeguards to strengthen protection from fraud, as there is no comparable EU legislation that could help to tackle problems such as financial fraud, identity theft, and ransomware attacks.

6.1.6.2 Option 1 - a voluntary approach

- A **voluntary approach (Option 1)** could be implemented in different ways, for instance relying on either national authorities, industry or a combination of the two to take steps to adopt good practices in the integration of security design and default considerations into the design and production of internet-connected RE products from the outset.
- A voluntary approach could either be implemented independently or could be used to support the effective implementation of a regulatory approach, i.e. to support the implementation of the delegated acts building on the **good practice guidance documents** developed to address security issues in respect of connected RE devices in the EU and the US. In parallel, both ENISA at EU level and NIST in the US have developed guidance on **minimum baseline security requirements.** Such guidance, whilst voluntary, has potential to help industry to improve current practices in terms of building in basic security functionality to internet-connected RE products and devices, which many already do, but not all.
- Industry associations were **generally in favour of an industry-led voluntary approach** (with some exceptions)**,** mainly because they did not to want to see additional legislation on data protection and privacy. These associations were concerned that there has been insufficient time to allow existing legislation to become fully embedded, as the GDPR came into force in May 2018 and the voluntary certification-based approach under the CSA was only adopted in June 2019 and has not yet been applied to any products.
- Several **manufacturing industry associations** expressed the view that the level of risk and probability of risks occurring and their impact had been somewhat exaggerated, beyond particular categories of high-risk product groups such as smart toys. They therefore suggested that whereas one or two higher risk product categories should be regulated, not all should be.
- However, the product-based case studies identified many examples of risks and security vulnerabilities that could lead to device penetration and data breaches. Some are common across all internet-connected RE products and devices, whilst others are specific to particular product

groups. Moreover, a wide array of academic research and grey literature points to many specific risks which does not suggest that a voluntary approach has been effective to date.

- Other stakeholders such as consumer associations, MSAs and many (but not all) national authorities, were against a voluntary approach as they suggested it would provide insufficient certainty for consumers and businesses, and could expose users of such products and devices to breaches of their personal data, leading to data protection and privacy being undermined, and exposing them to fraud risks.
- Some stakeholders, particularly industry and manufacturing associations, defended a non-regulatory approach through the **development of voluntary codes of practice** that complement the implementation of mandatory requirements.
- While all stakeholders welcomed the voluntary initiatives to promote good practices and to strengthen awareness of cybersecurity through the development of good practice guidance (e.g. DCMS code of conduct) and the development of baseline security requirements (e.g. by ENISA at EU level and NIST in the US), consumer associations and many national authorities argued that there has been insufficient progress by manufacturers of internet-connected RE products and devices (especially cheaper consumer IoT devices) in strengthening attention to ensuring basic security functionality is integrated into product design and manufacturing.
- A voluntary approach would only be effective if there were to be much more active engagement by industry, standards organisations and national authorities to work together through a partnership-based approach to ensure that security vulnerabilities in internet-connected RE products are tackled. If a voluntary approach were to be decided upon, this could be based on a product group by product group approach, building on the framework provided by the CSA, coordinated by ENISA under the overall responsibility of the Commission's DG CONNECT.
- Overall, a voluntary approach alone is unlikely to be effective, and some regulators globally have already questioned whether it will be sufficient to ensure policy objectives (i.e. the UK and the US).

6.1.6.3 Options 2, 3 and 4 – a regulatory approach under the RED (Article 3(3)(e) and Article 3(3)(f)).

- Overall, three main regulatory gaps were identified that could justify a regulatory approach were identified.

  1. MSAs cannot remove products from the market (or prevent them being placed on the market) under the RED, and can only rely upon DPAs issuing fines under the GDPR (and in future the e-PR once this comes into effect in EU law). Therefore, non-compliant products remain on the market, undermining the Single Market.
  2. There are no requirements relating to data protection and privacy in instances where device manufacturers are not intending to collect and process data and therefore remain outside the GDPR's scope.
  3. There is presently no EU legislation explicitly addressing protection from fraud. National criminal legislation addresses fraud but only retrospectively, which could undermine the Single Market, as there is no EU legal framework to prevent fraud taking place as a result of device penetration. Given the increasing prevalence of fraud perpetrated by third parties accessing personal data unlawfully through , consumers arguably need greater preventive legal protection.

- Several policy options were analysed relating to the possibility of a regulatory approach through the activation of one or both of the delegated acts within study scope.
- Consumer associations, market surveillance authorities, and many (but not) all national authorities and cybersecurity agencies favoured a regulatory approach through the activation of

either one or both delegated acts (Article 3(3)(e) and Article 3(3)(f)).

- However, many industry associations and economic operators were not in favour of activating the delegated acts, due to concerns that it could be administratively burdensome to activate regulatory requirements relating to data protection and privacy, when there are already requirements under the GDPR and e-PD that if not complied with could lead to fines being issued by DPAs. There were also concerns that any additional essential requirements could require third-party and internal testing costs to check for compliance with harmonised technical standards. There was a concern as to the possible duplication of costs if for example, firms were already involved in voluntary ICT security certification schemes under the CSA were not able to use testing results to demonstrate compliance. However, this concern could be overcome if the harmonised standards drafted for the new essential requirements contain relevant technical requirements that have been identified in the voluntary certification under the CSA.

- Taking the options individually, **Option 2, activating Article 3(3)(e) only (data protection and privacy)**, was seen as complementary to the GDPR by stakeholders, especially consumer associations, national authorities and MSAs. However, this depends how the Delegated Act is written. It would evidently need to take as a starting point the overarching legal framework in place through the GDPR, aligning the delegated act under this Article was seen as being straight forward compared with Article 3(3)(f), as there is already EU legislation in place which defines key concepts such as data protection, privacy and consent.

- Given the legal characteristics of delegated acts, which serve to define detailed measures to support the implementation of legislation, if Article 3(3)(e) were to be activated, its scope would necessarily be **delineated by the definitions of data protection and privacy in existing EU legislation, namely the GDPR.** Furthermore, coherence and complementarity with the GDPR must be ensured.

- Turning to **Option 3, Article 3(3)(f), protection from fraud,** as there is no existing legal framework to underpin the implementation of this Article, turning this delegated act into a mandatory essential requirement was viewed as being more challenging. The absence of a definition of fraud in the RED was noted, although several examples as to what might constitute fraud in an IoT context, such as financial fraud and identity theft, were identified and analysed.

- Although some stakeholders argued that fraud should be tackled through national criminal legislation, such legislation is national (and heterogeneous providing uneven protection for users) rather than part of the Single Market. Moreover, criminal law tackles the problem retrospectively, whereas the problem of online frauds, including those resulting from internet-connected RE devices (and / or the data contained on, or transmitted from them) being compromised) has been growing. An argument was made by national authorities and MSAs that activating Article 3(3)(f) would be more effective by tackling the problem in the design phase to prevent the problem from occurring in the first place.

- Regarding **Option 4, activating both Delegated Acts** under **Article 3(3)(e) and Article 3(3)(f) respectively,** stakeholders that were supportive of a regulatory approach favoured the activation of both delegated acts at the same time. The rationale was that Article 3(3)(e) and 3(3)(f) are closely inter-related, and the distinction between the two is not always clear. There could be consequences of artificially dividing up data protection and privacy, and protection from fraud, as both would need to be addressed in parallel in the development of technical standards wherever possible to avoid two sets of costs being incurred, one for data protection and privacy and the other to prevent fraud.

- A regulatory approach would only be effective if suitable harmonised technical standards were to be developed, building on existing international and industry standards.

- Many of the security vulnerabilities identified could be addressed if encryption and authentication capabilities were to be implemented in internet-connected RE devices. However, whilst these would form the basis for protecting device penetration and data breaches, even end-to-end encryption and authentication cannot provide cast-iron guarantees, as some malware may be developed that can unencrypt data and/ or other technologies may be developed capable of penetrating encrypted data.

- A regulatory approach will therefore only be effective if technical standards are kept under regular review, such that manufacturers could address security vulnerabilities relating to the device's hardware/ operating system and software. Moreover, to be fully effective, software and app's downloaded onto devices would need to fall within the same regulatory regime, as otherwise the device may be compliant with security requirements under the RED at the point when placed on the market, but expose users to vulnerabilities once on the market, if for example, the device can be penetrated by compromising third-party software and app's. Whereas the legal framework focuses on pre-product placement, in practice, a more holistic approach is needed if security vulnerabilities are to be addressed such that personal data and privacy and protection from fraud could be ensured during the lifecycle.
- A regulatory approach under the RED may only be effective if supported by accompanying measures, such as awareness-raising on cybersecurity issues among consumers, manufacturers and other economic operators in the value chain regarding how data protection and privacy can be safeguarded and protection from fraud better ensured.
- Whilst there is strong awareness among leading global manufacturers and brands, without raising levels of security awareness among all actors using internet-connected RE products, technological solutions on their own, are unlikely to resolve the problems identified fully. This is because users themselves may expose a device to data loss and / or fraud, even if the manufacturer takes all reasonable steps to ensure that the device (or data contained therein) cannot be penetrated by unauthorised third parties.

6.1.6.4 Option 5 - Strengthening cybersecurity under dedicated horizontal legislation

- A potential fifth policy option could be to consider the introduction of a horizontal piece of legislation on cybersecurity applicable to all connected and non-connected devices and products (to avoid discriminating between connected RE and wired products without a direct or indirect internet connection). Some cybersecurity specialists stated that whilst there are additional risks stemming from products being connected, devices that are not connected in any way, but are non-secure, still present a risk. However, a horizontal approach was only seen as being realistic over the medium term.
- Although not originally envisaged in the study scope, many key stakeholders, in particular from industry, noted that horizontal legislation may be a more effective regulatory approach in the medium term to ensure a level regulatory playing field between wireless products subject to the RED, which would be subject to new essential requirements under the delegated acts, and wired products, which would be exempt in the interim period. Covering wireless connected products would indeed leave some gaps in that would not cover wired internet connectivity e.g. broadband via cable, DSL, etc. However, it would at least cover an estimated 70% of the market.
- Furthermore, these stakeholders view strong cybersecurity as a key pre-requisite for the protection of personal data and privacy, and protection from fraud. This is evidenced by the fact that, although concepts such as data protection by design and default are detailed in existing legislation, most of the technical literature and good practice guidelines focus on security by design and default. However, this policy option is only achievable in the medium term, given the time it would take to consult on, develop and negotiate such a legislation.
- Other stakeholders however advocated adopting an incremental approach starting by activating the two DA and then incrementally aligning other relevant industrial product legislation with these

requirements.

6.1.7 Impacts

- Overall, strengthening cybersecurity for RE-connected devices through a regulatory approach by activating both delegated acts within scope (alongside software potentially, as otherwise this would leave a gap, given value chains for complex products) could have positive economic, social and environmental impacts.
- Macro-economic benefits could be achieved under several sub-options, but particularly under a regulatory approach, since this would ensure higher levels of trust among consumers in IoT devices, products and services, leading to higher sales.
- Further economic benefits could be realised by ensuring that manufacturers are obliged to ensure that products address basic cybersecurity functionality requirements from the design process, since this would reduce substantive compliance costs for manufacturers, compared with a situation in which they faced regulatory uncertainty, but continued reputational management risks in the case of scandals pertaining to lack of cybersecurity in connected RE products.
- From a societal perspective, social benefits of enhancing consumer trust in IoT would include a reduction in unnecessary risks for IoT consumers, with less chance of their personal data and privacy being compromised, and a reduced likelihood of fraud (although clearly, unlike technical solutions to ensure physical product, there are limits to how secure devices can be from a cybersecurity perspective given the evolving nature of vulnerabilities and threats).
- Turning to environmental benefits, there was a perception that eliminating low-cost, but low-quality, non-compliant products from the market could lead to less consumption of very cheap electronic products by European consumers.
- Due to the sheer scale of growth in internet-connected RE products and devices, and limited resources among MSAs, there are already many products on the European market that are non-compliant with the RED’s existing essential requirements, and which moreover do not adhere to basic security functionality principles either. This was seen as having an adverse impact on the European market by undermining the competitiveness of compliant manufacturers, be they European or international.
- The benefits evidently vary depending which policy option is concerned. For example:
  - Some stakeholders argued that the benefits of a regulatory approach would include greater legal certainty for manufacturers and consumers, and a reduced likelihood of consumer detriment due to higher levels of trust in consumer IoT. This was seen in turn as strengthening the full economic potential of the Digital Single Market.
  - Conversely, other stakeholders argued that either strengthening the effectiveness and enforcement of existing EU legislation or adopting a non-regulatory approach could bring about similar benefits, through improved cybersecurity. A further suggested benefit of not legislating was seen as being the avoidance of additional administrative costs, with greater flexibility for IoT device manufacturers, and reduced risks of duplicating regulation.
  - However, consumers would have less legal protection under a voluntary approach (either through the CSA or industry-led initiatives), therefore there would be less certainty that the expected social benefits would materialise to the same extent. This aspect is difficult to assess however, as if the GDPR were to be implemented and enforced effectively, then a voluntary approach could also be effective by complementing existing legislation.

6.1.8 Cost-benefit assessment (CBA)

An assessment of the costs and benefits (CBA) was undertaken, focusing on quantification of the costs of a regulatory approach, but taking account of all the policy options.

Nature and extent of costs

- Some industry associations and their members were concerned that the introduction of mandatory requirements could lead to greater costs for manufacturers, such as the need to integrate authentication into products and to procure secure chips and components.
- This could in turn lead to a risk that costs would be passed on to consumers for some connected RE products, leading to moderately higher prices.
- Whilst encryption and authentication were seen as being effective means of safeguarding products from a data protection and privacy perspective, as well as in the prevention of fraud, these were not always seen as being needed for simpler connected RE products, especially if some internet-connected RE devices and products collect very limited or no personal data.
- However, research into Willingness to Pay suggests that consumers would be willing to pay slightly more to ensure their connected RE products are secured, and that personal data and privacy are protected. Indeed, large firms and multinationals already invest in product security to prevent data breaches and sometimes integrate this into their branding and value proposition.
- Some economic operators were also concerned about how the essential requirements that would emanate from the activation of the delegated act might be implemented. In particular, the concern relates to whether these would cover all, or only specific categories of RE-connected products, and the associated costs of compliance, depending on which types of products the DAs would be applicable to.
- Several industry associations and economic operators (targeted consultations) were concerned that costs are difficult to anticipate until industry sees the detail of the delegated acts and harmonised technical standards that could be developed if a standardisation mandate were to be issued to the ESOs by the Commission.
- The scale of administrative compliance costs – were the two delegated acts to be activated – was found to vary depending on factors such as sales volume and the ability to absorb costs through low compliance costs per unit, the extent of in-house testing capacity, which determines whether a given IoT device manufacturer has to use an external third-party testing laboratory (irrespective as to whether legally required or 'voluntary').
- If either or both of the delegated acts under the RED were to be activated, SMEs could be more affected in terms of administrative compliance costs than larger firms, as they generally produce in lower volume of production and therefore face higher average compliance costs per unit.
- There were challenges in obtaining compliance costs data from individual firms, due to the absence of detailed information about how the delegated acts would be developed, or what minimum baseline security requirements harmonised technical standards will consist of. For example, it is as yet not known whether more generic standards based on common sense security by design principles (e.g. approach in the ETSI standard on consumer IoT), or more technical, detailed and product-specific.
- Nevertheless, some examples of different types of costs were identified. Internal and especially external testing costs were found to be one of the main types of costs that could be incurred by RE equipment manufacturers and other economic operators in the value chain e.g. chip manufacturers and electronic components suppliers (EEE).
- One of the factors that needed consideration in quantifying costs was the nature of data being collected by smart products, whether this involves personal data, data with identifiers that could be construed as personal data, or non-personal data, such as device to device data sharing among internet-connected RE devices and products, machine-to-machine data sharing, etc.
- The scope of a possible delegated act on data protection and privacy (Art. 3(3)(e) would need to

take as a starting point the definitions in the GDPR (Art. 5) in delineating what types of data would fall within scope. The assessment of costs could therefore be updated once the delegated acts have been drawn up, as presently there are many different variables that remain uncertain.

- If a regulatory approach were to be adopted, manufacturers would incur some substantive compliance costs in new product development. However, in many cases, these would be mitigated as many costs would have occurred anyway through Business as Usual costs i.e. among good practice manufacturers, ensuring basic security functionality is part of the product design and manufacturing process. MSAs also highlighted that implementing baseline security requirements and ensuring basic cybersecurity features does not imply major product engineering.
- There were however divergent views as to what these costs would entail. Some stakeholders argued that this was more a question of changing purchasing behaviours by equipment and appliance manufacturers that integrate cheap chips for connectivity functionality and them instead procuring other types of chips. It was argued that chips offering security functionality are available on the market for broadly the same price as unsecure chips, and it is therefore more a question of encouraging cultural change among chip manufacturers to offer secure products systematically to their manufacturing customers.
- However, some stakeholders pointed out that in a post-GDPR world, it is unrealistic for manufacturers to avoid consideration of minimum baseline security requirements in connected RE and wearables, as consumers expect IoT devices to integrate safeguards into product design to ensure basic cybersecurity functionality as a precursor for ensuring data protection and privacy and protection from fraud.
- Many of the substantive compliance costs that would occur under a regulatory approach can be attributed as BaU costs. Since consumers are increasingly concerned about security vulnerabilities, manufacturers of internet-connected RE devices and products will have to strengthen attention to ensuring basic security functionality, regardless as to whether there are additional legislative requirements or not, to protect their reputation and manage risks. Data breaches not only risk fines under the GDPR, but can do significant reputational damage, with very high costs for the firm concerned.
- Some stakeholders attested to the close inter-relationship between data protection and privacy and protection from fraud under Article 3(3)(e) and 3(3)(f) respectively. However, equally, it was suggested that there may be instances where data protection and privacy is compromised without a clear risk of fraud or vice versa, and therefore there is a rationale for specifying these separately, even if from an administrative costs perspective, testing costs would be reduced if technical standards developed were to address these in parallel rather than separately.

Assessment of benefits

- Considering the nature and extent of benefits that could arise from improved security and safeguards in internet-connected RE products and devices in respect of data protection and privacy and protection from fraud, some stakeholders argued that the net impact of introducing mandatory baseline security requirements could also lead to an overall reduction in costs, due to the minimisation of the hidden costs of non-secure products remaining on the market, such as the reputational damage that non-secure products have on the rest of the economic operators that produce secure products, reducing the economic and societal costs of data breaches, etc.
- Data breaches are costly for both users who lose their personal data and risk fraud but also manufacturers and other economic operators associated with the product. For example, in 2019, IBM and the Ponemon Institute placed the average total cost of a data breach at $3.92m and the UK Home Office estimated the cost of cyber-crime to be £1.1bn in 2015/16.
- The types of costs linked to data breaches for companies include: i) direct costs, such as non-

compliance fines (e.g. under GDPR or the proposed e-Privacy Regulation) and costs directly attributable to the breach itself and post breach activities; and ii) indirect costs, such as reputational damage and loss of customers. In addition, certain direct (e.g. money lost due to financial fraud etc.) and indirect costs (e.g. reduced confidence in the security of RE devices) are borne by consumers and businesses. Improving the security of internet-connected RE devices and products therefore has the potential to reduce costs. Moreover, the economic and societal costs of non-action could be significant.

- Improving the security of internet-connected RE devices and products could also reduce the risk of manufacturers incurring significant fines. Some large fines have already been issued under the GDPR as a result of insufficient security practices, including three specifically related to Article 25 GDPR (data protection by design and by default).
- Although some costs estimates have been developed (Section 5.3.3), it is clear that a number of aspects related to security and the costs of data breaches in general, as well as in consumer and enterprise IoT, are difficult to quantify. In particular, this includes the indirect, long term and intangible costs, such as the impact of the loss of trust in IoT devices.
- There are concerns regarding the risk of duplication in testing products to meet different regulatory requirements (e.g. the GDPR, e-PD and, where manufacturers are also participating voluntarily in certification schemes, the voluntary CSA). However, if the Commission drew up the DAs in a way that took into full account all existing EU legislation, and allowed compliance with other legislation, such as the GDPR and the certification schemes to be taken into account so as to avoid retesting, this could help to avoid an unnecessary burden being placed on industry.
- Whilst some substantive costs were identified, these were found to be outweighed by the scale of potential benefits, which include scope for higher demand among European consumers for IoT products due to increased trust in the security of consumer IoT products and devices.

6.2 Recommendations

6.2.1 Recommendations from the IA study

Recommendation 1: The preferred policy option (Option 4) would be to activate both delegated acts under Article 3(3)(e) and 3(3)(f) of the RED. This would strengthen the RED's essential requirements to close regulatory loopholes, and making an explicit link between product safety and security (data protection and privacy and protection from fraud).

Recommendation 2: All internet-connected RE should be brought within scope to strengthen security in respect of data protection and privacy and protection from fraud. However, there are two options for the Commission in implementing the future delegated acts under the above-mentioned Articles.

- Under the first Option, all internet-connected RE devices and products should be brought within the scope of the delegated acts from the outset.
- Under the second Option, an incremental approach should be adopted based on activating the two DAs followed by gradually bringing more products within scope over time, based on a risk-based assessment. *Reference should be made to the product-based assessment of security vulnerabilities, risks and the likelihood of these occurring.*

Recommendation 3: The European Commission should issue a standardisation mandate to the European Standardisation Organisations (ESOs) pertaining to the two delegated acts. Mapping by the ESOs to date (e.g. ETSI, CENELEC) suggests that there are already a lot of technical solutions to build upon, although there are also challenges as some existing standards relate to generic security measures rather than product-specific solutions.

Recommendation 4: The ESOs should work closely with industry in developing harmonised technical standards and build on existing technical solutions and industry standards where these already exist. This would minimise potential future compliance costs for industry of ensuring safeguards relating to the security of internet-connected RE and wearable RE, with a focus on data protection and privacy and protection from fraud.

Recommendation 5: The requirements under the RED Art. 3(3)(e) and Art. 3(3)(f) will need to be clearly delineated in the drafting of the delegated acts, and supported by a clear explanation as to how in the case of Art. 3(3)(e) coherence will be ensured with existing legal obligations in respect of data protection and privacy in EU legislation (e.g. the GDPR, and the e-PD / e-PR). Clear definitions are provided in the GDPR in respect of key concepts such as data protection, privacy, consent, data subject, etc. These already help to provide protection for users of internet-connected RE, and these definitions could lay the basis for the development of the activation of the delegated acts, which would need to be aligned with the GDPR.

Recommendation 6: Duplication of costs between the RED and other EU legislation should be avoided. To assuage manufacturers' concerns regarding administrative compliance costs (especially due to testing and conformity assessment procedures), the extent to which compliance processes carried out by manufacturers under existing legislation and under voluntary certification schemes within the CSA could be used to demonstrate compliance towards the RED's essential requirements under future harmonised technical standards should be made clear.

Recommendation 7: Regular monitoring of new and emerging security vulnerabilities and threats should be carried out by ENISA on behalf of the European Commission. ENISA already has experience in monitoring and mapping security vulnerabilities. ENISA, and possibly also working groups from relevant national authorities, could advise the Commission on whether harmonised standards still represent the state-of-the-art.

Recommendation 8: Regular discussions on how best to address security vulnerabilities in internet-connected RE and wearable RE - including the role of harmonised technical standards - should take place regularly within the framework of the Commission's Radio Equipment Expert Group (RE EG).

Recommendation 9: Greater attention should be given to monitoring the implementation and strengthening the enforcement of existing EU legislation with the potential to contribute to regulatory objectives linked to Article 3(3)(e) and 3(3)(f) of the RED to ensure ongoing coherence. There should be a focus on further strengthening compliance by manufacturers of internet-connected RE and wearable RE with certain Articles of the GDPR that are especially relevant, such as Art. 25 (security by design / default). If DPAs were to issue fines to non-compliant manufacturers, then over time, a combination of such fines and case law could help to further embed compliance.

Recommendation 10: A study on the GDPR's on internet-connected RE and wearables from a data protection and privacy perspective should be undertaken in future. This would help to develop a better evidence-based understanding as to how far GDPR has already led to changes in business processes and the embedding of security features in products at the design, engineering and manufacturing stages to ensure higher levels of data protection and privacy.

Recommendation 11: Good practice sharing among manufacturers that already take security by design and default, and their data protection by design and default obligations seriously (including their integration into business processes) should be identified, collected and shared in the form of good practice guidance.

6.2.2 Further strategic recommendations

Looking ahead, this study to support an IA raises a number of issues study that would benefit from possible follow-up through targeted actions. This section briefly presents some broader strategic recommendations, based on the IA findings.

Continued monitoring of the effectiveness of the existing EU legislative framework. The GDPR provides an extensive rulebook for the protection of personal data, including by manufacturers of connected RE devices. However, there are regulatory gaps. For instance, the legislation is not tailored to industrial products and does not provide legal powers for MSAs to remove products that do not adequately protect the personal data of users from the market (although supervisory authorities have other powers, such as the possibility of issuing fines and notices). It is therefore recommended that one or more of the following actions could be considered:

i. Draw on the findings from future evaluations of the existing legislative framework, in particular the GDPR, which is due for evaluation by 25 May 2020 (as per Art. 97(1)) and every subsequent four years.

ii. Conduct a standalone study to examine the impacts of the GDPR and other relevant legislation on the protection of personal data by manufacturers of industrial products, more generally, or specific of connected RE products. This would then help to ensure that any feedback from industry regarding challenges in implementing GDPR in an IoT context. This could then inform the possible drawing up an implementation of delegated acts under the RED.

Furthermore, it will be important to ensure that those involved in the ongoing negotiations over the **ePrivacy Regulation consider the perspective of manufacturers of connected RE products** in the context of the proposed Regulation to ensure that the links between the ePR and the two delegated Acts in the RED (pertaining to data protection and privacy) are sufficiently clear. Presently, the draft points to these being mutually exclusive.

Ongoing monitoring of security vulnerabilities in connected RE products that could lead to data protection and privacy being compromised or data breaches leading to fraud.

The Commission should **collect up to date information at EU and national level about security vulnerabilities that could lead to data breaches and risk personal data / privacy being compromised and frauds perpetuated.** Data could be collected either by the Commission (or by a delegated organisation such as ENISA) on a real-time basis as to:

- What types of vulnerabilities have been identified in connected RE products;
- The scale and prevalence of vulnerabilities; and
- The costs and impacts associated with dealing with these.

ENISA is already responsible for monitoring security vulnerabilities under the CSA. Their remit could be extended to include the delegated acts under the RED for any vulnerabilities specific to data protection and privacy and protection from fraud. This could be used to help assess the effectiveness of regulatory (or any non-regulatory) measures to address the problem in future. This could also help to inform the assessment of different types of vulnerabilities, the risks of these occurring and the impacts associated with different classes of connected RE products. If an incremental approach were to be adopted to the RED's implementation, information on security vulnerabilities would be crucial to inform its implementation.

Moreover, the **vulnerability disclosure policies** stipulated in the CSA could provide a useful model to facilitate a structured process of cooperation in which vulnerabilities are reported to the owners of information systems about particular product groups. These are meant to be reported on a voluntary basis at national level within individual sub-sector agreements. Data about vulnerabilities could be fed back to manufacturers and other economic operators to raise awareness about vulnerabilities and technical solutions to address these. A name and shame approach should be avoided, as the intention would be to encourage a **culture of good practice and information sharing about vulnerabilities and potential (effective) technical solutions** between relevant actors with a view to better monitoring and responding to emerging vulnerabilities at European level and globally that could be factored in by manufacturers to product design, covering security, data protection and privacy by design and default.

Engage industry in the journey towards secure internet-connected RE products. In the stakeholder consultations, some industry stakeholders, such as industry representative associations and individual manufacturers were not in favour of the activation of the two delegated acts

There are a number of **challenges industry faces regarding implementation of the existing EU legal framework in respect of data protection and privacy**. Among manufacturers, communication between legal experts and technical experts as to how they might meet their legal obligations under the EU legislative framework is difficult because there is a need for practical guidance as to what actions should be taken to implement the law effectively. Several stakeholders pointed to the difficulty that technical engineers working on IoT product compliance and lawyers working with the GDPR do not speak the same language and see compliance issues differently. This is complicated by the rapid development of new technologies used in data collection processing and gathering, such as machine learning, artificial intelligence and big data analytics.

As such, irrespective of whether the delegated acts are activated, engagement with industry to drive the adoption of good practices in securing connected RE products is of importance. Although leading manufacturers are already implementing security by design and default as a good practice in parallel with documenting business processes to show how they have implemented technical and organisational measures under the GDPR relating to data protection by design and default. However, the culture of security by design and default should be spread more widely to include all economic operators in the value chain, including ODMs and OEMs, as if they are not data processors themselves, they fall outside the GDPR's scope.

Good practices in implementing baseline security into connected RE should be highlighted, as well as examples of effective approaches to compliance with data protection by design and default requirements under the GDPR.

Annex 1 - Bibliography

A bibliography is provided below of the documentation that has been consulted. This includes the following types of literature:

- EU legislation, impact assessments and guidance on the RED;
- Horizontal developments in the applicable requirements across industrial product legislation (e.g. through the New Legislative Framework and Alignment Package);
- Data and statistics on radio equipment products;
- Studies, research reports and other publications on GDPR, privacy and data protection in an IoT context and on cybersecurity; and
- Grey literature (articles, blogs and white papers) on related topics.

Country	Year	Title and abstract (where relevant)	Authors
EU legislation, impact assessments and guidance on the RED and horizontal developments in the applicable requirements across industrial product legislation			
EU	2019	Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Adopted on 12 February 2019, Version of Public Consultation	European Data Protection Board (EDPB)
EU	2018	Opinion 5/2018 – Preliminary Opinion on Privacy by Design	European Data Protection Supervisor (EDPS)
EU	2018	Guide to the Radio Equipment Directive 2014/53/EU, Version of 05 June 2018	European Commission
EU	2018	Publication in accordance with Article 1(3) of the Commission Decision 2000/299/EC (Version January 2018)	European Commission
EU	2017	Commission Implementing Regulation (EU) 2017/1354 of 20 July 2017 specifying how to present the information provided for in Article 10(10) of Directive 2014/53/EU of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1354 Although different from Art. 3(e) and 3(f), this shows potentially the mechanism through which particular further regulatory objectives could be achieved before goods are placed on the market.	European Commission
EU	2017	Goods Package - proposed strengthening of the overall regulatory framework on market surveillance. Proposal for a regulation - COM(2017)795/DOCUMENT-2017-82474 https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-795_en	European Commission
EU	2017	Proposal for a Directive of the European Parliament and Council on Combatting Fraud and Counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA	European Commission
EU	2017	Proposal for a Regulation of the European Parliament and of the Council – on the Mutual Recognition of goods lawfully marketed in another Member State	European Commission2014
EU	2016	Article 45 of the RED establishes the Telecommunication Conformity Assessment and Market Surveillance Committee (TCAM), a committee related to Regulation (EU) No 182/2011. https://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en	European Commission and Telecommunication Conformity Assessment and Market Surveillance Committee (TCAM)
EU	2014	Directive 2014/53/EU 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 Text with EEA relevance,	European Parliament and The Council of the European Union

Country	Year	Title and abstract (where relevant)	Authors
		https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053	
EU	2012	Commission Staff Working Document, Impact Assessment on the RED, Brussels, 17.10.2012, SWD(2012) 329 final https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012SC0329	European Commission
EU	2012	Commission Staff Working Document, Executive Summary to the Impact Assessment, Brussels, 17.10.2012, SWD(2012) 329 final https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012SC0300	European Commission
EU	2011	Impact Assessment Board Opinion, DG ENTR - Impact Assessment on: Proposal for a revision of the R&TTE Directive http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2012/sec_2012_0567_en.pdf	European Commission
EU	2011	Regulation (EU) No 182/2011 of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers	European Commission
EU	2014 / 2018	Official Guide to the Radio Equipment Directive 2014/53/EU – Version December 2018 Manual for all parties directly or indirectly affected by the Radio Equipment Directive 2014/53/EU (RED). It should assist in the interpretation of the RED but cannot take its place; it explains and clarifies some of the most important issues related to the Directive's application. The Guide also aims to disseminate widely the explanations and clarifications reached by consensus among Member States and other stakeholders.	European Commission
General EU legislation on data protection and privacy			
EU	2019	**The Cybersecurity Act.** 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	The European Parliament and The Council of the European Union
US	2018	**Senate Bill No. 327, Chapter 886,** Part 4 of the Division 3 of the Civil Code relating to Information Privacy	State of California – Legislative Council Bureau
EU	2016	**The GDPR – Regulation (EU) 2016/679** of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en The previous Article 29 Working Party issued some opinions which might be relevant in the context of this study, such as Opinion 02/2013 on apps on smart devices. Further opinions and position papers on particular relevant articles of GDPR will be reviewed.	European Parliament and The Council of the European Union
EU	2002	**ePrivacy Directive (ePD)** – Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	European Parliament and the Council of the European Union

Country	Year	Title and abstract (where relevant)	Authors
		https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058	
EU	2017 (and 2019 drafts)	**ePrivacy Regulation (e-PR).** https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation **The** ePrivacy Directive needs to be adapted to align with new rules in the GDPR. The regulation would replace the e-PD but has not yet been adopted.	
Literature on data protection by design and default, security by design and default and on relevant legislation in an IoT context (GDPR, ePrivacy Directive and Regulation)			
UK (EU-focused)	2019	**The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 – October 2019** Contains a chapter on GDPR implementation including commentary on the implementation of data protection by design and default. https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1209988/european-union-overview	
EU	2018	**GDPR Best Practices - Implementation Guide Transforming GDPR Requirements into Compliant Operational Behaviours. –** **https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000** Publication sets out best practices in GDPR compliance. Notes that one of the biggest challenges for organisations that fall within the broad extra-territorial scope of GDPR, is transforming the legal requirements of the GDPR into compliant and sustainable operational behaviours.	Metacompliance
UK	2020	**The impact of IoT security labelling on consumer product choice and willingness to pay. PLOS ONE. 15. e0227800. 10.1371/journal.pone.0227800.** The study involved a behavioural economics experiment and adopted a willingness to pay approach to the IoT and covers IoT products such as smart TVs, smart watches, WiFi routers, Security Cameras and Thermostats. The study was funded by the Engineering and Physical Sciences Research Council (Award EP/N02334X/1) and the Dawes Centre for Future Crime at UCL.	Blythe, J.M., Johnson, S.D. & Manning, M. Wong. G
UK	2020	**What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices.** Crime Sci 9, 1 (2020). https://doi.org/10.1186/s40163-019-0110-3	Blythe, J.M., Johnson, S.D. & Manning, M.
UK	2019	**The GDPR and the Internet of Things: A Three-Step Transparency Model** The IoT requires pervasive collection and linkage of user data to provide personalised experiences based on potentially invasive inferences. Consistent identification of users and devices is necessary for this functionality, which poses risks to user privacy. The forthcoming General Data Protection Regulation (GDPR) contains numerous provisions relevant to these risks, which may nonetheless be insufficient to ensure a fair balance between users' and developers' interests. A three-step transparency model is described based on known privacy risks of the IoT, the GDPR's governing principles, and weaknesses in its relevant provisions. Eleven ethical guidelines are proposed for IoT developers and data controllers on how information about the functionality of the IoT should be shared with users	Sandra Wachter

Country	Year	Title and abstract (where relevant)	Authors
		above the GDPR's legally binding requirements. Two use cases demonstrate how the guidelines apply in practice: IoT in public spaces and connected cities, and connected cars.	
FI	2018	**'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' 26 (2018) International Journal of Law and Information Technology 45–63.** https://academic.oup.com/ijlit/article-abstract/26/1/45/4769343 The increasingly complex data-processing reality created by new technologies, such as the 'Internet of Things' (IoT) underline the need for stakeholders to be clear about issues relating to responsibility for the personal data they process and/or control. The European General Data Protection Regulation (GDPR) expands the obligations of data processors and brings changes to the relationships between IoT stakeholders. To understand how the law operates in an IoT context, we need to analyse the complexity of the current legal state and map out grey areas. The focus of this article lies mainly on the contractual relationship between controllers and processors dealing with new technology, and changes to data controllers' and data processors' rights and obligations brought by the GDPR. The main aim is to investigate whether the GDPR is fit to deal with new technologies such as the IoT.	Jenna Lindqvist
UK	2016	**Holloway, Donell & Green, Lelia. (2016). The Internet of toys. Communication Research and Practice.** The Internet of Toys refers to a future where toys not only relate one-on-one to children but are wirelessly connected to other toys and/or database data. While existing toy companies and start-ups are eagerly innovating in this area, problems involving data hacking and other privacy issues have already occurred. The Hello Barbie and VTech hacks in late 2015 are recent examples. This article reviews, outlines, and analyses these recent advances in children's engagement with the Internet. It shows how Internet-connected toys, among other data-inducing practices (such as baby wearables and school analytics), are implicated in big data processes that are datafying a generation of youngsters. Significant issues exist around the data security and safety of The Internet of Toys for child consumers who are usually too young to fully understand and consent to data collection or to understand other security issues. http://www.tandfonline.com/doi/abs/10.1080/22041451.2016.1266124	Holloway, Donell & Green, Lelia.
EU	2017	**Mascheroni, G., & Holloway, D. (Eds.) (2017). The Internet of Toys: A report on media and social discourses around young children and IoToys. DigiLitEY.** http://digilitey.eu/wp-content/uploads/2017/01/IoToys-June-2017-reduced.pdf Examines the discursive environment of smart toys, i.e. its representations in media commentaries and commercial advertisements. Also frames privacy as a Children's Right. Points to scandals involving smart toys in 2016, in particular the fact that some toys were *"using speech-recognition technology to enable voice interactions with children, and consumer protection organizations brought claims that the*	Giovanna Mascheroni & Donell Holloway

Country	Year	Title and abstract (where relevant)	Authors
		company was saving these voice recordings. These recordings could then be shared with unspecified third parties without giving parents and caregivers adequate warnings". There were also concerns about hidden marketing practices.	
FI	2016	**'The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges'.** Data Protection, Privacy and European Regulation in the Internet Age (Forum Iuris, Helsinki 2016) 84-109.	Jenna Lindqvist Tobias Bräutigam & Samuli Miettinen (eds.)
UK	2018	**Big data analytics, consent and the European Union (EU) General Data Protection Regulation 2016 (GDPR) - The fallacy of consent and control, Joel Padi, Keele University, 2018.** The EU GDPR is meant to put data subjects in control of their personal data in the face of 21st century data processing, characterised by 'big data analytics'. The ability to consent to or reject the processing of personal data is widely regarded as a data subject's primary mechanism of controlling their personal data under the GDPR. This paper analyses the GDPR's ability to safeguard the utility of a data subject's consent, thus, control over their personal data on its application to 'big data analytics'. As a result of its analysis, this paper finds the GDPR's formulation of consent to be inapplicable to big data analytics and incapable of putting data subjects in control of their personal data. Accordingly, this paper investigates and ultimately rejects the utility of existing supplementary mechanisms of regaining control of personal data. The paper concludes with the proposition of an abstract regulatory framework designed to supplement the GDPR and safeguard a data subject's control over their personal data in the face of big data analytics.	Joel Padi
FI	2015	**'Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things' (2015) Information & Communications Technology Law 24/3, 262-277.** **https://www.tandfonline.com/doi/abs/10.1080/13600834.2015.1091128** The technology used to provide connectivity from anytime, any place and for anyone. Now anything can be added to the list. In the 'IoT', the amount of individuals' data collected and processed is increasing substantially as data are being collected from various sources. Most communications between smart devices occur automatically, potentially without the user being aware of it. Many questions arise around the vulnerability of the devices in the IoT, often deployed outside a traditional IT structure and lacking sufficient built-in security. The IoT demands consideration and research into how to best balance the opportunities that the IoT affords against legal risks it imposes on data protection. Considerable questions about how our currently existing EU framework for protection of personal data applies in IoT are being raised. The data protection legislation needs to move from theory to practice and in order to achieve this; the legal framework may need additional mechanisms.	Jenna Mäkinen
EU	2017	**Reform of the ePrivacy Directive - EU legislation in Progress European Parliament Briefing** http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf	Shara Monteleone

Country	Year	Title and abstract (where relevant)	Authors
		In January 2017, the Commission tabled a proposal for a regulation on privacy and electronic communications to replace the current 2002 ePD. The main objectives of the review are: enhancing security and communications confidentiality; defining clearer rules on tracking technologies such as cookies; and achieving greater harmonisation among Member States. Stakeholders are divided on certain issues, including on the basic need for a new measure to protect confidentiality in e-communications.	
EU	2013	**Data Protection by Design and Technology Neutral Law. Computer Law & Security Review, Vol. 29, No. 5, 2013, p. 509-521.** Argues that to achieve a technology neutral law, technology-specific law is sometimes required. Discriminates between three objectives, often implied in the literature on the technological neutrality of law. The **compensation objective** refers to the need to have technology-specific law in place whenever specific technological designs threated the substance of human rights. The **innovation objective**, referring to the need to prevent legal rules from privileging or discriminating specific technological designs in ways that would stifle innovation. The **sustainability objective** refers to the need to enact legislation at the right level of abstraction, to prevent the law from becoming out of date too soon. The relevance of the three objectives is illustrated regarding the EU cookie Directive (2009). The salience of the legal obligation of Data Protection by Design and Default in the GDPR is explained and tested against compensation, innovation and sustainability objectives.	Hildebrandt, Mireille; Tielemans, Laura
UK	2017	**Security and privacy in the internet of things** **Pages 155-184 | Received 20 Apr 2017, Accepted 08 Jul 2017, Published online: 24 Aug 2017** https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1366536?src=recsys The IoT is a technology that has the capacity to revolutionise the way we live, in sectors ranging from transport to health, from entertainment to interactions with government. This opportunity also presents significant challenges. The growth in the number of devices and speed of growth presents challenges to our security and freedoms as we battle to develop policies, standards, and governance that shape this development without stifling innovation. This paper discusses the evolution of the IoT, its various definitions, and some of its key application areas. Security and privacy considerations and challenges that lie ahead are discussed both generally and in the context of these applications.	Carsten Maple
NL	2011	Demetrius Klitou (2011**), Privacy by Design and Privacy-Invading Technologies: Safeguarding Privacy, Liberty and Security in the 21st Century**, Legisprudence, 5:3, 297-329, DOI: 10.5235/175214611799248904	Demetrius Klitou
US	2018	**China's Internet of Things, October 2018** The IoT is being applied to virtually every sector from smart thermostats in households to swarms of autonomous drones in the battlefield. This report, contracted by the USCC and authored by SOS International, outlines China's state-led approach to IoT development, assesses the implications for the U.S. economy, national security, and	John Chen, Emily Walz, Brian Lafferty, Joe McReynolds, Kieran Green, Jonathan Ray, and James Mulvenon - Research Report Prepared on Behalf of the U.S.-China Economic and Security. Review Commission,

Country	Year	Title and abstract (where relevant)	Authors
		the privacy of U.S. data, and makes recommendations for U.S. policymakers. China's concerted, state-led approach, including ongoing efforts to influence international IoT standards, has put China in a position to credibly compete against the United States and other leaders in the emerging IoT industry. China's research into IoT security vulnerabilities and its growing civil-military cooperation raise concerns about gaining unauthorized access to IoT devices and sensitive data. In addition, China's authorized access to the IoT data of U.S. consumers will only grow as Chinese IoT companies leverage their advantages in production and cost to gain market share in the United States based on the terms of use and sweeping Chinese government data access powers.	
	2009	**Ann Cavoukian, Privacy by Design. Take the Challenge (Ontario: Information and Privacy Commissioner of Ontario (Canada), available at https://ozone.scholarsportal.info/bitstream/1873/ 14203/1/291359.pdf**	
DE/ UK	2007	**Comparison of Privacy and Trust Policies in the Area of Electronic Communications.** https://www.academia.edu/27046343/Comparison_of_Privacy_and_Trust_Policies_in_the_Area_of_Electronic_Communications	Authors: wik-Consult: J. Scott Marcus, Kenneth CarterRAND Europe: Neil Robinson, Lisa Klautzer, Chris MarsdenCLIP: Joel Reidenberg, Camilla Abder, Cedric Burton, Lisa Cooms, Ezra KoverCRID: Yves Poullet, Florence De Villenfagne, Franck DumortierGLOCOM: Adam Peake, Keisuke Kamimura, Tazuko Tanaka
	2014	**Internet Privacy Rights - Rights to Protect Autonomy.**	Bernal, Paul
	2019	**DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?** AI poses fundamental questions concerning its ethical, social and legal impact thus setting new challenges to privacy and data protection. Since 2016, many reports and legislative initiatives have appeared to consider and address the impact of artificial intelligence on society and law. Does AI accelerate the erosion of data protection and related fundamental rights or is there room for mitigating risks and preventing the adverse consequences of an "amplified" AI? Is GDPR applicable to AI? The GDPR applies both in the phase of AI development and with regard to its use for analyzing and decision-making about individuals. The provisions of GDPR with regard to the rights of data subjects, the obligations deriving from accountability or the obligations of processors will contour the way AI and machine learning will be developed and applied. Moreover, the GDPR comprises the elements to face technological transformations. One of the tools in this regard consists of Data Protection Impact Assessments (DPIA) that have to be carried out before the deployment of high-risk technologies. A second tool, strictly interrelated to DPIA is the duty to protect personal data by design that the GDPR compels to data controllers.	Lilian Mitrou
UK		**International Data Privacy Law. British Information Commissioner's Office, 'Big Data and Data Protection'** https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-dataprotection	ICO, UK

Country	Year	Title and abstract (where relevant)	Authors
UK	2017	**Data Protection Act and General Data Protection Regulation - Big data, artificial intelligence, machine learning and data protection, 2017.** https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf Discussion paper looks at the implications of big data, artificial intelligence (AI) and machine learning for data protection, and explains the ICO's views on these. The ICO starts by defining big data, AI and machine learning, and identifying the particular characteristics that differentiate them from more traditional forms of data processing. After recognising the benefits of big data analytics, the main implications for data protection are analysed.	
US	2013	**What Is Privacy Worth? University of Chicago Law School,** Source: The Journal of Legal Studies, Vol. 42, No. 2, pp. 249-274 https://www.cmu.edu/dietrich/sds/docs/loewenstein/WhatPrivacyWorth.pdf Understanding the value that individuals assign to the protection of their personal data is of great importance for business, law, and public policy. We use a field experiment informed by behavioral economics and decision research to investigate individual privacy valuations and find evidence of endowment and order effects. Individuals assigned markedly different values to the privacy of their data depending on (1) whether they were asked to consider how much money they would accept to disclose otherwise private information or how much they would pay to protect otherwise public information and (2) the order in which they considered different offers for their data. The gap between such values is large compared with that observed in comparable studies of consumer goods. The results highlight the sensitivity of privacy valuations to contextual, nonnormative factors.	Author(s): Alessandro Acquisti, Leslie K. John, and George Loewenstein
	2009	**Privacy, Data protection, and the Unprecedented Challenges of Ambient Intelligence, Paper accepted for publication in Studies in Ethics, Law and Technology** https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 Privacy and data protection are identified as complementary legal instruments aimed at protecting respectively the individual's possibility to construct his own identity and personality without undergoing unreasonable constrains, and the individual's ability to control some aspects of their identity.	Dr Antoinette ROUVROY, Information Technology & Law Research Centre, University of Namur, Belgium
		To Track or 'Do Not Track' Advancing Transparency and Individual Control in Online Behavioral Advertising Study about online tracking.	Omer Tene and Jules Polonetsky
FI	2018	**Personal Data Protection on The Internet of Things, an EU Perspective.** PhD thesis. The ('IoT' has become an important part of major cities' infrastructure, where quality of life is improved by, for example, connected healthcare, transport, and parking. The IoT is also present in homes where the technology is used for homeautomation, such as automated heating, -lighting, or -appliances. People also use smart devices to monitor their health and daily activities. Along with the increasing use of smart technology, personal data are often collected and recorded, and they can, for example, be used to derive the location of	Jenna Lindqvist, Faculty of Law, University of Helsinki, Finland

Country	Year	Title and abstract (where relevant)	Authors
		a person's home or workplace, to monitor habits and lifestyle, or to target advertisement based on the data subject's interests. As the traditional Internet has developed into the IoT, personal data protection law has also expanded from being a niche field of law, into a legal area that is applicable in almost all sectors, services, and technologies. Globalisation and vast technological development, and elaborated collection of data, raised questions about whether current EU data protection legislation can cope with the new challenges that the IoT poses. Issues identified by the European Commission include: a need to more clearly define how the data protection principles apply to new technologies; the need for harmonisation between EU MS' data protection legislation; a need for additional regulation of data processors; and the need of better ensuring enforcement of data protection rules. The IoT poses challenges to personal data protection mainly because the amount of personal data that is collected has increased substantially, and because information is gathered from so many different, scattered sources. In addition, the form of automatic communication between smart devices makes it difficult to apply fundamental transparency and fairness principles. This dissertation investigates the complexity of the legal state in EU surrounding personal data protection in the context of the IoT. The articles forming the dissertation outline changes both in law, and the world at large, point out legal unclarities, and contribute to the academic discussion about the possible effects of the GDPR. In a nutshell, this study aims to answer the question: Is the GDPR fit to deal with new technologies such as the IoT?	
		Protecting vulnerable groups - Child Privacy Protection Online: How to Improve It through Code and Self-Regulatory Tools	Federica Casarosa
Data and statistics on radio equipment products			
US	2018	"IoT in Consumer Electronics Market Research Report-Global Forecast to 2023" – Market Analysis, Scope, Stake, Progress, Trends and Forecast to 2023. https://www.marketresearchfuture.com/sample_request/997	
US	2017	IoT in Europe: Market opportunities and main applications http://www.reportlinker.com/p05043293/IoT-in-Europe-Market-opportunities-and-main-applications.html Offers a thorough study of the size of the IoT market and different strategies of telecom operators in the European region	
EU	2016	Study for DG CNCT by Tech4i2 on the **"Identification of the market for radio equipment operating in licence-exempt frequency bands to assess medium and long-term spectrum usage densities"** This document reports on a study to identify the market for radio equipment operating in licence-exempt (LE) frequency bands within the 400 MHz to 6 GHz range to assess spectrum usage densities to 2030.	Report undertaken by Tech4i2 – publicly available
NL	NA	The Internet of Things in Europe, https://www.cbi.eu/node/2668/pdf/ CBI is part of the Netherlands Enterprise Agency and are funded by the Netherlands Ministry of Foreign Affairs.	
Studies, research reports and other publications on Consumer IoT security			

Country	Year	Title and abstract (where relevant)	Authors
EU	2019	**ETSI Technical Standard in Consumer IoT – TS 103 645** TS 103 645 was published on 19 February 2019 and is the world's first globally-applicable standard for consumer IoT security. The document specifies high-level provisions for the security of consumer devices that are connected to network infrastructure, such as the Internet or home network, and their associated services. A The document provides basic guidance for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. It provides cybersecurity provisions for consumer IoT, such as the avoidance of universal default passwords, implementing a means to manage reports of vulnerabilities, securely store credentials and security-sensitive data, ensuring that personal data is protected and making the installation and maintenance of devices easier. Available from : **https ://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf**	ETSI, Technical Committee on Cybersecurity
EU	2019	**Data Breach Investigations Report (DBIR)** This report is built upon analysis of 41,686 security incidents, of which 2,013 were confirmed data breaches. We will take a look at how results are changing (or not) over the years, as well as digging into the overall threat landscape and the actors, actions, and assets that are present in breaches. Windows into the most common pairs of threat actions and affected assets are also provided. 194	Verizon
NL	2019	**Strict – Report on IoT Device Security (Onderzoek veiligheid apparaten).** Addresses IoT device security. This covered 22 IoT consumer devices across different product groups, such as internet routers, connected toys, IP cameras, smart locks, baby monitors and smart thermostats. The study investigated the extent to which the software of these devices adheres to the principles of 'Security by Design', 'Security by Default', 'Privacy by Design' and 'Privacy by Default'. This was done by performing a scan for vulnerabilities in the software, analysing the standard configuration and looking at communication flows. Investigation was also done to check what types of data the devices collect, how the data is stored and how the suppliers handle this data, according to their privacy statements. Where possible, recommendations were made with improvements. Four of the 22 devices were classified as having 'critical' security vulnerabilities. Four and nine out of the devices had findings for which the level of security vulnerabilities was identified as being 'high' or 'medium'. https://www.agentschaptelecom.nl/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur	Strict on behalf of the Radiocommunications Agency Netherlands
US	2011	802.11x Vulnerabilities, Attacks and Solutions https://www.giac.org/paper/gsec/1959/80211x-vulnerabilities-attacks-solutions/103413	David C. Weiler, Global Information Assurance Certification Paper

Country	Year	Title and abstract (where relevant)	Authors
UK	2019	In May 2019, UK govt. dept. DCMS published an online consultation on consumer IoT[209]. This includes consideration as to whether a regulatory or a non-regulatory approach would be optimal to complement the earlier initiatives of the development of an industry code of practice. Three options are outlined, relating to the possible use of mandatory security and secure by design labelling. The consultation paper recognises the "urgent need to move the expectation away from consumers securing their own devices and instead ensure that strong cyber security is built into these products by design".	
US	2019	**Core Cybersecurity Feature Baseline 2 for Securable IoT Devices: A Starting Point for IoT Device Manufacturers** This relates to the development of baseline security requirements through the US standards organisation NIST. Specifically, NIST IR 8259. This publication is intended to help Internet of Things (IoT) device manufacturers understand the cybersecurity risks their customers face so IoT devices can provide cybersecurity features that make them at least minimally securable by the individuals and organizations who acquire and use them. The publication defines a core baseline of cybersecurity features that manufacturers may voluntarily adopt for IoT devices they produce. The baseline addresses general cybersecurity risks faced by a generic customer. Manufacturers often know more about their customers and the risks they face, so the publication also provides information on how manufacturers can identify features beyond the core baseline most appropriate for their customers and implement those features to further improve how securable their IoT devices are. This approach could help to lessen the cybersecurity-related efforts needed by IoT device customers, which in turn should reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised IoT devices.	Authors – Michael Fagan, Katerina N. Megas, Karen Scarfone, Matthew Smith
EU	2018	**Good Practices for Security of Internet of Things in the context of Smart Manufacturing, ENISA, November 2018.** ENISA study aims at addressing the security and privacy challenges related to the evolution of industrial systems and services precipitated by the introduction of IoT innovations. The main objectives were to collect good practices to ensure security of IoT in the context of Industry 4.0/Smart Manufacturing, while mapping the relevant security and privacy challenges, threats, risks and attack scenarios. Available from: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot	ENISA
EU	2018	**What the Internet of Things means for Consumer Privacy** What the Internet of Things means for consumer privacy discusses the findings of an Economist Intelligence Unit (EIU) research programme, sponsored by ForgeRock, that explores the privacy concerns and priorities of global consumers stemming from the Internet of Things (IoT) and	The Economist Intelligence Unit

[209] https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security

Country	Year	Title and abstract (where relevant)	Authors
		related technologies. At the core of the research is a global survey of 1,629 consumers that The EIU conducted in October 2017. Respondents come from eight countries: Australia, China, France, Germany, Japan, South Korea, the UK and the US. They fall into six age groups ranging from 16 to over 65, and the sample is divided evenly among men and women.	
UK	2018	**Code of Practice for Consumer IoT Security.** Code of Practice to support all parties involved in the development, manufacturing and retail of consumer IoT with a set of guidelines to ensure that products are secure by design and to make it easier for people to stay secure in a digital world. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf	Department for Digital, Culture, Media & Sport (DCMS) in conjunction with the National Cyber Security Centre (NCSC)
UK	2018	'Secure by Design: Improving the cyber security of consumer Internet of Things: Report', https://www.gov.uk/government/publications/secure-by-design	Department for Digital, Culture, Media & Sport (DCMS)
UK	2018	Guidance – Consumer guidance for smart devices in the home, Updated 14 October 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747624/Consumer_Guidance_for_Smart_Devices_in_the_Home_Oct_2018.pdf	Department for Digital, Culture, Media & Sport (DCMS)
UK	2018	Summary literature review of industry recommendations and international developments on IoT security, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686090/PETRAS_Literature_Review_of_Industry_Recommendations_and_International_Developments_on_IoT_Security.pdf	PETRAS IoT Hub. Commissioned by the Department for Digital, Culture, Media & Sport (DCMS)
UK	2018	Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security, October 2018 Maps the Code of Practice for Consumer IoT Security against published standards, recommendations and guidance on IoT security and privacy from around the world. Around 100 documents were reviewed from nearly 50 organisations. Whilst not exhaustive, it represents one of the largest collections of guidance available to date in this area. The purpose of the mapping is to serve as a reference and tool for users of the Code of Practice. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf.	Department for Digital, Culture, Media & Sport (DCMS)
FR	2018	« L'Internet des objets 2018 – Marchés, Technologies, Cybersécurité »	Société de l'électricité, de l'électronique et des technologies de l'information et de la communication)
International	2018	Smart But Unsafe: Experimental Evaluation of Security and Privacy Practices in Smart Toys, September 2018, https://arxiv.org/pdf/1809.05556.pdf	Sharon Shasha, Moustafa Mahmoud, Mohammad Mannan, and Amr Youssef
EU	2017	**Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, ENISA.**	ENISA

Country	Year	Title and abstract (where relevant)	Authors
		The report elaborates baseline cybersecurity recommendations for IoT with a focus on Critical Information Infrastructures, which encompass facilities, networks, services and physical and information technology equipment. These infrastructures are considered critical because their destruction or disruption could bring about major consequences for the health, safety and economic wellbeing of citizens, for the efficient functioning of State institutions and Public Administrations5,6, and for the asset owners who make use of IoT to provide their services. Available from : https ://publications.europa.eu/en/publication-detail/-/publication/c37f8196-d96f-11^{e}7-a506-01aa75ed71a1	
EU	2017	**JRC Technical Reports, Kaleidoscope on the Internet of Toys, Safety, security, privacy and societal insights** This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf	Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. Stéphane Chaudron, Rosanna Di Gioia, Monica Gemo, Donell Holloway, Jackie Marsh, Giovanna Mascheroni, Jochen Peter, Dylan Yamada-Rice
EU	2017	**Securing consumer trust in the internet of things – Principles and Recommendations.** Publication by European and International Consumer Associations which examines different ways of promoting enhanced consumer trust.	ANEC, BEUC, Consumers International
EU	2017	**WatchOut, Analysis of smartwatches for children, October, 2017** https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf	Norwegian Consumer Council (Forbrukerrådet)
FR	2017	L'Internet des Objets : état des lieux et perspectives – DSIH – http ://www.dsih.fr/images/Rapport-etude_IoT_ARUBA-1.pdf	Hewlett Packard Enterprise
IT	2017	Internet delle cose. Dati, sicurezza e reputazione., ISBN : 9788891759139 https ://www.francoangeli.it/Ricerca/scheda_libro.aspx ?CodiceLibro=1304.3	Reputation Agency, Isabella Corradini. Contributi : Corrado Giustozzi, Alessandra Smerilli, Luca Rossetti, Corradino Corradi, Massimo Simeone, Marilena Tardito, Giampaolo Fiorentino, Carmela Occhipinti
Brazil	2017	Security Requirements for Smart Toys http://www.scitepress.org/Papers/2017/63370/63370.pdf	Luciano Gonçalves de Carvalho and Marcelo Medeiros Eler, School of Arts, Sciences and Humanities, University of São Paulo, Brazil, FATEC Mogi das Cruzes, São Paulo State Technological College, Brazil DOI: 10.5220/0006337001440154, In Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017) – Volume 2, pages 144-154, ISBN: 978-989-758-248-6

Country	Year	Title and abstract (where relevant)	Authors
			Copyright © 2017 by SCITEPRESS– Science and Technology Publications, Lda. All rights reserved,
International	2017	Computing in Smart Toys, International Services on computer entertainment and Media Technology, https://books.google.co.uk/books?id=K4wwDwAAQBAJ&pg=PA146&lpg=PA146&dq=Smart+watches+and+Smart+toy+studies&source=bl&ots=pyJf6EYAZ9&sig=Fpoxyo_IaRF8KkDAUqZTqyCN8eg&hl=en&sa=X&ved=2ahUKEwj3oYz-gJDeAhUMPsAKHTQ9Ajc4KBDoATAIegQIAhAB#v=onepage&q&f=false	Springer International Publishing, edited by Jeff K.T. Tang, Patrick C. K. Hung
EU	2017	Europeans' attitudes towards cyber security, Eurobarometer Report 464a This report brings together the results of the Special Eurobarometer public opinion survey towards cyber security in the 28 European Union countries.	European Commission, Directorate-General for Migration and Home Affairs and co-ordinated by Directorate-General for Communication
US	2017	Security& Privacy in Smart Toys https://www.utdallas.edu/~juniavalente/valente17iotsp2.pdf	Junia Valente, Alvaro A. Cardenas, Erik Jonsson School of Engineering& Computer Science, The University of Texas at Dallas {juniavalente, alvaro.cardenas}@utdallas.edu
US	2017	Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys http://techpolicylab.org/wp-content/uploads/2016/01/Toys-That-Listen_CHI-2017.pdf	Emily McReynolds, University of Washington, Seattle, WA, USA, Sarah Hubbard, University of Washington, Seattle, WA, USA, Timothy Lau, University of Washington, Seattle, WA, USA , Aditya Saraf, University of Washington, Seattle, WA, USA, Maya Cakmak, University of Washington, Seattle, WA, USA, Franziska Roesner, University of Washington, Seattle, WA, USA
US	2016	Future of Privacy Forum – Family Online Institute (FOSI), Kids & the connected home: privacy in the age of connected dolls, talking dinosaurs and battling robots, 2016 https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf	Future of Privacy Forum (FPF) and Family Online Safety Institute (FOSI)
US/ DE	2016	Finding Europe's Edge in the Internet of Things https://www.bain.com/insights/finding-europes-edge-in-the-internet-of-things/	Bain and Company, Michael Schallehn, Michael Schertler and Christopher Schorling
US	2015	EY, Cybersecurity and the Internet of Things, 2015 https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf	Points out that the IoT will increasingly rely on cloud computing, and smart devices with sensors built in, along with thousands (if not millions) of applications to support them. The problem is that the integrated environments needed to support connected technologies do not exist, and cloud computing is in need of serious improvement, especially in security terms.
EU	2015	Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses	Annika Bergström

Country	Year	Title and abstract (where relevant)	Authors
EU	2013	Future Identities: Changing identities in the UK – the next 10 years - DR 19: Identity Related Crime in the UK This review has been commissioned as part of the UK Government's Foresight project, Future Identities: Changing identities in the UK – the next 10 years. The purpose of this paper is to explore the regulative challenges that identity crimes pose for the public, policymakers and law enforcement. The paper accompanies DR20 The Future Challenge of Identity Crime in the UK (Wall, 2013) which considers the broader context, politics and futures of Identity Crime. Both papers contribute to the Government Office for Science Foresight project that is investigating how changes in technology, geo-politics, demographics and economics over the next 10 years might affect notions of identity and subsequently impact on behaviour.	David S. Wall, Durham University for the UK Government's Foresight Project
Costs of Data Breaches			
Global	2018	**2018 Cost of a Data Breach Study: Global Overview,** IBM Security and Ponemon Institute, July 2018 https://www.ibm.com/downloads/cas/861MNWN2 Interviews with more than 2,200 IT, data protection, and compliance professionals from 477 companies that have experienced a data breach over the past 12 months.	
US	2018	**rIoT - Quantifying Consumer Costs of Insecure Internet of Things Devices** Kim Fong, Kurt Hepler, Rohit Raghavan, Peter Rowland, University of California, Berkeley, School of Information. https://pdfs.semanticscholar.org/7396/8dfe4ab7c885ab5d7b51815d3b25d8d92640.pdf This report focuses on the former—exploiting vulnerable devices for their computing power and ability to use their network's bandwidth for cyberattacks—specifically DDoS attacks on Internet domains and servers. Insecure Internet-connected devices create widespread costs, both direct and indirect, among a variety of stakeholders, including network targets, device manufacturers, Internet service providers (ISPs), and consumers (Anderson et al., 2013; Federal Trade Commission, 2015, pp. 10-18). Identifying the targets on the receiving end of botnet DDoS campaigns is often easier than identifying other affected stakeholders because targets incur the most visible costs. The rise of markets for services like cyber insurance and DDoS protection, moreover, create economic incentives to focus on the costs to targets, which may lose millions of dollars due to downtime during an attack (Osborne, 2017; Matthews, 2014; Romanosky, 2017).	
UK	2018	**Understanding the costs of cyber crime,** A report of key findings from the Costs of Cyber Crime Working Group, Research Report 96, Home Office Science Advisory Council, January 2018	Costs of Cyber Crime Working Group
UK	2019	**2019 Cyber Security Breaches Survey (CSBS),** National Cyber Security Agency. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf	

Country	Year	Title and abstract (where relevant)	Authors
		Sought to gather costs data on the costs and impacts of cyber breaches and attacks on UK organisations	
	Grey literature on costs of data breaches	https://www.techrepublic.com/article/data-breaches-now-cost-companies-an-average-of-1-41-million/ http://iotsecurityconnection.com/posts/how-data-breaches-are-hitting-consumer-wallets https://www.ul.com/insights/making-connection-between-iot-security-and-brand-trust https://www.itprotoday.com/iot/report-iot-security-breach-costs-smaller-firms-13-percent-annual-revenue https://digitalguardian.com/blog/whats-cost-data-breach-2019 https://www.idquantique.com/2019-cost-of-a-data-breach-report/	
Grey literature (articles, blogs and white papers)			
US	2019	**Whitepaper - HOW TO SOLVE THE 6 TOP SECURITY CHALLENGES OF EMBEDDED IOT DESIGN** Ensuring security for embedded IoT designs can be challenging and time-consuming, even for veteran developers. Explore these six common security challenges in hardware and software, and delivers in-depth, comprehensive defences with multiple layers of protection. An estimated 31billion IoT devices will be deployed by 2020, many with limited security controls and hacking risks. Why are so many embedded systems designed with vulnerabilities? In large part, it's because developers face multiple challenges and complexities when securing embedded applications and devices. Available at: https://theinternetofthings.report/Resources/Whitepapers/c1051a68-493c-4347-8569-d9fc84afbb9a_iot-security-whitepaper.pdf	Renesas Electronics Corporation
US	2019	**Whitepaper - IoT cybersecurity guidelines, standards and verification systems,** Currently there is no recognized international IoT cybersecurity standard to which IoT device manufacturers can conform. This leaves manufacturers without a label or customer-facing recognition program that they can leverage to promote their cybersecurity credentials.	Khan, Faud & Rogers, David, Caba.
US	2019	**Whitepaper - Core Cybersecurity Feature Baseline for Securable IoT Devices** This publication aims to improve how securable IoT devices are. IoT device manufacturers are given advice as to how they can help IoT device customers with cybersecurity risk management.	
	2019	**Surveillance capitalism and children's data: the Internet of toys, D Holloway, 2019.** Expresses concerns that the emergence of Internet-connected toys and things for children will amplify children's position as data sources under surveillance capitalism. https://journals.sagepub.com/doi/full/10.1177/1329878X19828205	D Holloway

Country	Year	Title and abstract (where relevant)	Authors
US	2018	Cyber risk in an Internet of Things world: Flashpoint edition 4: More data, more opportunity, more risk. The IoT offers new ways for businesses to create value, however the constant connectivity and data sharing also creates new opportunities for information to be compromised. Explore some of the more notable developments in the battle to combat cyber risks. https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html	Deloitte, Irfan Saif, Deloitte Risk and Financial Advisory Principal
UK	2018	Article, SMART TOY REVENUES TO GROW BY ALMOST 200% FROM 2018 TO $18 BILLION BY 2023, May 2018 https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-grow-by-almost-200	Juniper Research
UK	2017	Which? Article - Smart toys - should you buy them? https://www.which.co.uk/reviews/smart-toys/article/smart-toys-should-you-buy-them	Which?, Andrew Laughlin
UK	2017	Article, Be Careful Buying a Smartwatch for Your Kid, 18 OCT 2017, https://uk.pcmag.com/news-analysis/91635/be-careful-buying-a-smartwatch-for-your-kid	PC Mag, MICHAEL KAN
EU	2017	News Article, Germany bans children's smartwatches, https://www.bbc.co.uk/news/technology-42030109	BBC, Jane Wakefield, Technology reporter
EU	2017	News Article, Child safety smartwatches 'easy' to hack, watchdog says, 18 October 2017, https://www.bbc.co.uk/news/technology-41652742	BBC, Joseph Venable, Technology reporter
UK/ ES	2017	**Whitepaper "Building a Trusted and Managed IoT World".** Whitepaper analyses the development of IoT security technologies, proposes the employment of multi-layered end-to-end security mechanisms to safeguard the IoT, and summarizes IoT security practices. IoT technologies are developing apace. However, they are vulnerable to new security issues and threats. The security of the IoT can be ensured only if the industry chain works together as a whole. Therefore, Huawei proposes that all governments, international organizations, and industries join hands to build IoT security and work harder in guiding policies, enacting laws and regulations, setting standards, innovating new technologies, and building industry ecosystems.	INCIBE, Red.es & Huawei
UK	2017	Article, Smart toy vulnerabilities could provide a way for hackers to watch and talk to children, Feb 17, 2017, https://www.techworld.com/security/could-hackers-use-smart-toys-watch-talk-children-3654839/	TechWorld, Thomas Macaulay
International	2018	Amazon purges creepy CloudPets smart toys amid privacy concerns https://www.theinquirer.net/inquirer/news/3033772/amazon-purges-creepy-cloudpets-smart-toys-amid-cyber-security-and-privacy-concerns	The Inquirer, Roland Moore-Colyer
International	2018	Blog, Industry must take action to improve connected toy security – part 1, May 21, 2018, HTTPS://WWW.TATACOMMUNICATIONS.COM/BLOG/2018/05/INDUSTRY-MUST-TAKE-ACTION-TO-IMPROVE-CONNECTED-TOY-SECURITY-PART-1/	Tata Communications, Srini CR, Chief Digital Officer
International	2018	BT article, Retailers drop CloudPets smart toys over cyber-security concerns, updated June 2018, http://home.bt.com/tech-gadgets/tech-news/retailers-drop-cloudpets-smart-toys-over-cyber-security-concerns-11364276692680	BT News Article

Country	Year	Title and abstract (where relevant)	Authors
UK	2019	Risks of internet-connected products and IoT devices being added to their network, which risk providing an easy entry point if not properly secured from attackers. Many IoT devices are built with limited security. If discoverable on the network, this poses cybersecurity risks as an entry point to the entire network. https://www.zdnet.com/article/iot-devices-pose-bigger-security-risks-than-most-realize/	ZNet
US	2017	Gifts That Snoop? The Internet of Things Is Wrapped in Privacy Concerns, December 13, 2017 https://www.consumerreports.org/internet-of-things/gifts-that-snoop-internet-of-things-privacy-concerns/	Consumer Reports, Bree Fowler
US	2017	When It Comes to Smart Toys, It Pays to Shop Smart, 24 November 2017 https://www.internetsociety.org/blog/2017/11/comes-smart-toys-pays-shop-smart/	Internet Society, Ryan Polk, Policy Advisor
UK	2017	12 ways to make connected smart toys safer, Article providing advice from Steve Wood, deputy commissioner for the ICO, an independent authority that upholds information rights in the public interest. https://parentzone.org.uk/article/12-ways-make-connected-smart-toys-safer	ParentZone
EU	2017	Significant security flaws in smartwatches for children, Publisert 18. oktober, 2017 https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/	Norwegian Consumer Council (Forbrukerrådet)
FR	2017	L'Internet des objets en pleine expansion, Le Monde - https://www.lemonde.fr/pixels/article/2017/06/08/l-internet-des-objets-en-pleine-expansion_5140586_4408996.html	
UK	2016	Smart teddy bear can be hacked to track children, https://www.telegraph.co.uk/technology/2016/02/03/smart-teddy-bear-can-be-hacked-to-track-children/	Telegraph
FR	2016	Les défis de l'Internet des objets, CNRS Le journal - https://lejournal.cnrs.fr/articles/les-defis-de-linternet-des-objets	
EU	2016	Article, Connected toys violate European consumer law, 6. desember, 2016 https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/	Norwegian Consumer Council (Forbrukerrådet)

Annex 2 – Key study issues: an analytical framework

Key study issues	
Problem definition and identification of needs	• What are the main threats and vulnerabilities for internet-connected radio equipment ("RE") and devices (e.g. smart watches / wearables, other types of equipment)? • Are there any examples of non-cyber-secure connected RE products that have been placed on the European Single Market that could expose users to risks as regards inadequate data protection and privacy and/ or lack of sufficient protection from fraud? How prevalent is the problem? • To what extent – if at all – can non-cyber-secure RE products be removed from the market by market surveillance authorities ("MSAs") using existing EU legislation? • To what extent is adequate attention being paid by manufacturers of consumer IoT devices to ensuring high levels of data protection and privacy? To what degree is there enough attention to ensuring protection from fraud? • If a problem in relation to non-cyber secure RE products can be identified, how significant is the problem? To what extent – and how - does it affect particular stakeholder groups (e.g. manufacturers, other economic operators and consumers)? • To what extent does the problem warrant policy intervention at EU level (either of a regulatory or non-regulatory nature)? • To what extent does existing EU legislation (e.g. GDPR, the ePrivacy Directive) provide adequate protection for consumers to ensure 1) data protection and privacy and 2) protection from fraud? • Are there any examples of either national regulations pertaining to ensuring data protection and privacy, or protection from fraud for IoT consumer products? • In which specific EU countries do such national regulations exist? Can any lessons be learnt to date from their implementation in terms of ensuring high levels of cybersecurity in consumer IoT products? • Are there any examples of effective non-regulatory approaches, such as voluntary codes of practice? If yes, are these led by government, industry or through a coordinated approach?
Optimal means of achieving regulatory objectives linked to data protection, privacy and fraud?	• What is the best way to achieve EU policy objectives? • Would the activation of the existing essential requirements in the RED foreseen under Art. 3(3)e and 3(3)f relating to data protection and privacy, and ensuring fraud prevention through enhanced cybersecurity be effective? • To what extent could a non-regulatory approach achieve similar objectives? Would there be any disadvantages and / or weaknesses of such an approach?
Definition of product groups within scope	• If two delegated acts (DA) were to be adopted pursuant to Article 3(3)(e) and Article 3(3)(f), which product groups should be included within scope within connected radio equipment? • What rationale could be given for the inclusion of either i) all RE product groups or ii) only selected specific product groups? Could it be justified that certain classes of internet-connected RE devices and wearables should be left out of the scope? If yes, on what grounds? • Do stakeholders agree with the provisional list of categories of radio equipment (including radio-connected toys, smartwatches and other wearables) which present similar technologies and/or similar risks developed by our study team?
Challenges and barriers to implementation of delegated acts	• Are there any potential challenges and barriers to the implementation of DA under the RED (Art. 3 e and 3f)? If yes, how best might these be overcome? For example: ▪ Are there any barriers to designing-in from the product design phase

Key study issues	
	strengthened data protection and privacy for end-users? ▪ Are there any particular challenges in designing-in enhanced cybersecurity features to address fraud risks from a manufacturers' perspective?
Costs and benefits	• What are the main costs and benefits associated with the policy options that have been defined? How do these differ between a regulatory and a non-regulatory approach? • To what extent can the administrative costs for manufacturers and economic operators be quantified? Are there also qualitative considerations that need to be factored into the CBA, such as the main cost drivers, variations depending on volume of production? • Are there likely to be differences in the administrative and substantive costs of compliance between large manufacturers and SMEs? How would this impact on fair competition and trade? If yes, how might any potential adverse impacts on SMEs be overcome? • What would be the main benefits of the different policy options? How do the benefits of a regulatory approach through the DA compare with existing legislation? And with a non-regulatory approach? • Do the findings in respect of costs and benefits suggest that regulatory intervention can be justified, through the activation of either one or two DA? Or is a non-regulatory approach also feasible if manufacturers design-in security features from the outset?
Impacts	**Impacts on the achievement of policy objectives** • To what extent would the adoption of one or both DA contribute towards the achievement of the Directive's two main objectives (promoting an internal market in radio equipment and ensuring high levels of safety)? • What is likely to be the impact on the functioning and harmonisation of the Internal Market if essential requirements relating to data protection and privacy and protection from fraud were to be activated? How does this compare with a non-regulatory approach? **Economic, social and environmental impacts and impacts by type of stakeholder** • What are likely to be the main impacts – economic, social and environmental – of going ahead with either one or both DA pursuant to Article 3(3)(e) and Article 3(3)(f) of the RED? To what extent can these be quantified? • To what degree would the adoption of the DA make products more convenient for consumers (e.g. protecting and ensuring the safety and security of children, enhancing trust among consumers in consumer IoT products)? • What would be the impacts on manufacturers and other economic operators across the value chain of the different policy options, in terms of the impacts on: ▪ SMEs, as opposed to large manufacturers; ▪ Electronic component and chip manufacturers, as opposed to equipment and household appliance manufacturers. ▪ Europe's industrial competitiveness across different categories of RE products (e.g. IoT consumer devices, smart toys and wearables?). • To what degree does the manufacturer's position within Global Value Chains ("GVC") influence the likely administrative and substantive costs of compliance were there to be a regulatory approach to strengthening cybersecurity pertaining to data protection and privacy and protection from fraud?

Key study issues	
Monitoring, market surveillance and enforcement arrangements	• If delegated acts pursuant to Art. 3(3)(e) and 3(3)(f) were to be adopted, what monitoring, market surveillance and enforcement arrangements need to be put in place to ensure effective monitoring of their implementation? • How would this be monitored by market surveillance authorities (MSAs) prior to market placement? • To what extent if the DAs were to be activated would this require joint cooperation between different regulatory bodies and other relevant stakeholders e.g. national data protection authorities and MSAs responsible for checking industrial products? • If the DAs were not activated and instead there was a reliance on existing EU legislation, such as the GDPR[210] and e-Privacy Directive (soon to be Regulation), to what extent would monitoring of the implementation of these regulation and directives need to be improved to look at implementation in an industrial products context?

[210] An example is Art. 25 of the GDPR, data protection by design and default.

Annex 3 - Interviews conducted

Organisation type	Completed (Interviewed)
Academic	5
Other private sector organisations (consulting firms, insurance companies in cybersecurity, cybersecurity firms)	4
Companies (SMEs)	8
EU Association	1
EU harmonised standards bodies & other standards and technical committees	2
EU Industry Association	14
EU institution/ EU body	3
European Consumer Associations	5
International consumer association	1
International industry association	1
Manufacturer	17
Market research	1
Market surveillance authorities	1
National Government	9
National Government (data protection)	2
Notified body	1
Testing & certification bodies	6
Total	**76**

Annex 4 – Checklist data protection and privacy by design and default

The GDPR's risk-based approach focuses on the concept of data controllers and processors demonstrating accountability, so as to show how they are complying with its requirements.

Example of a checklist relating to the implementation of principles relating to data protection and privacy by design and default to achieve GDPR-compliance

- We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- We make data protection an essential component of the core functionality of our processing systems and services.
- We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
- We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.
- We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
- We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.
- When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.
- We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

Source: Information Commission's Office (ICO) in the UK.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Annex 5 – Forecasts for internet-connected radio equipment

See separate standalone annex.

Annex 6 – Analysis of targeted consultation responses

See separate standalone annex.

Annex 7 – Analysis of OPC consultation responses

See separate standalone annex.

Annex 8 – Product-based case studies

See separate standalone annex.