Centre for Strategy & Evaluation Services

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

## Analysis of responses to the targeted consultation

April 7th, 2020

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

## Tables



## Figures

# 1. Introduction

## 1.1 Purpose of the consultation

This report presents the findings from a targeted consultation of stakeholders regarding the likely costs and benefits of activating two delegated acts pursuant to Articles 3(3)(e) and (f) of the Radio Equipment Directive (RED).[1] The RED establishes a regulatory framework for placing radio equipment on the market, ensuring a Single Market for radio equipment. The scope of the RED concerns devices that use the radio spectrum for communication and/or radio determination purposes. All internet-connected wireless devices (e.g. Internet of Things) fall under this Directive. However, with the increasing number of radio equipment placed on the market and with the continuing growth of the "internet of things" (IoT), the European Commission considers it a priority to increase legal certainty for consumers, manufacturers and other stakeholders.

The targeted consultation formed part of a wider study to provide input for the impact assessment accompanying a new initiative on internet-connected radio equipment and wearable radio equipment. It collected the specialist view of the different categories of stakeholders, such as industry associations, companies (including SMEs), consumers, enforcement authorities, etc, taking into account their different level of engagement and experience with the measure. The consultation was available from 3rd August to 15th November 2019 on the Commission's tool "EUSurvey".

In parallel to the targeted consultation, an open public consultation (OPC) was operated, which was open to any interested party. The results of the OPC are the subject of a separate report (Annex 7).

## 1.2 Implementation of the consultation

Stakeholders were invited to participate in the targeted survey, including those that have taken part in the Radio Equipment Expert Group meeting. Of these, 56 chose to respond by completing the questionnaire. It should be noted that the selected stakeholders were free to respond or not respond, so the sample has a degree of self-selection and is not necessarily representative of the overall cohort of stakeholders. The results presented here cannot be interpreted as those of a survey but rather as the expression of the opinion of a number of stakeholders with an interest in the legal framework relating to radio equipment devices. A number of responses across multiple respondents contained significant repetition, suggesting a co-ordinated response.

The online questionnaire consisted of both open and closed questions. The statistics stemming from the closed questions are presented here in the form of tables and charts. The answers to the open questions have been analysed thoroughly and used to complement a number of quantitative answers. However, since the open questions were optional and only a minority of respondents answered them, the responses to open questions have been used exclusively in a qualitative way (with no statistics derived), in order to illustrate certain phenomena with more detail or to exemplify suggestions for improvement. Some quoted comments have been translated from the source language or edited for reasons of grammar or spelling. Some questions required respondents to offer a score against a scale of 1 to 5. In these cases, 1 represented the highest score (e.g. "high level of concern", "significant risk/impact") and 5 presented the lowest score (e.g. "low level of concern", "no risks at all").

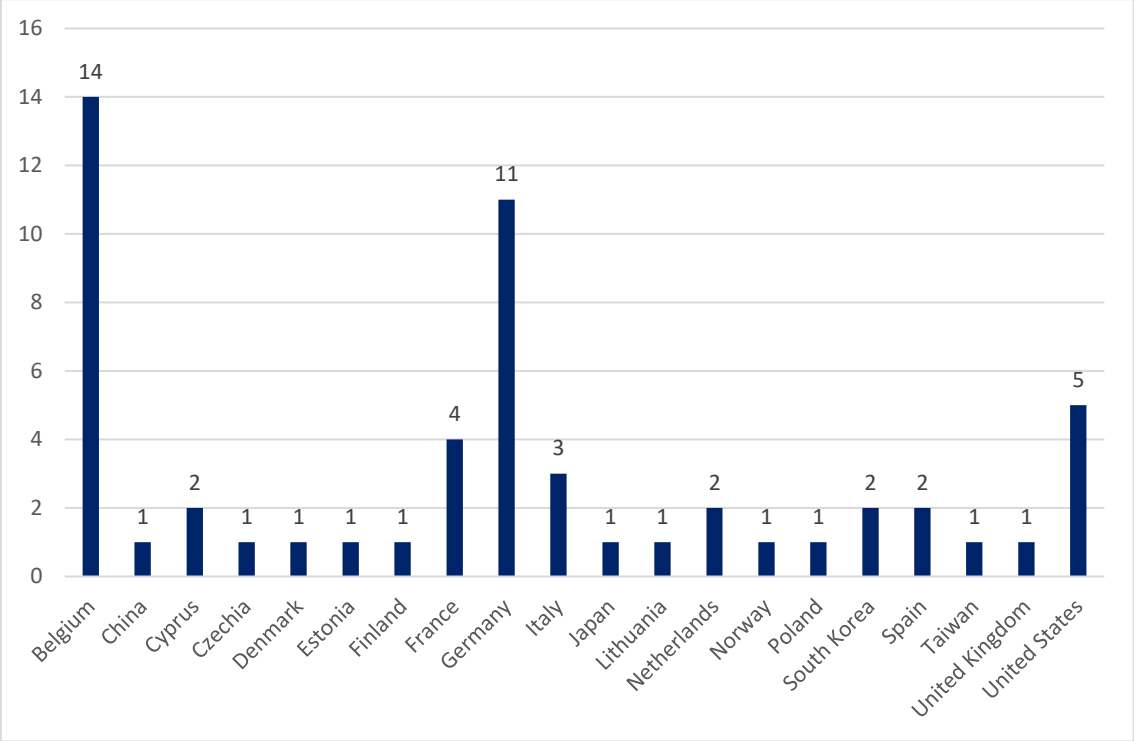
[1] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

# 2. Profile of respondents

## 2.1 Country of origin

The 56 respondents came from 20 countries, including 14 EU Member States. The largest number of responses (14) came from Belgium, nearly all of which were bodies representing manufacturers or consumers. Germany was the next best represented country with 11 respondents, most of which were manufacturers. Of the non-EU Member States, the USA was best represented with 5 respondents, which included a mix of manufacturers and industry bodies.

**Figure 1: Respondents' country of origin**




## 2.2 Type of organisation

A majority of the 56 respondents consisted of supply-side organisations, namely manufacturers, economic operators and their representative organisations or associations. Just less than one-fifth (10) were national public administrations, whilst 7 were compliance assessment bodies. Two were consumer organisations, whilst two others were academic institutions. The three "other" respondents consisted of a law firm, a technical expert and a regulation impact assessment consultant.

**Figure 2: Type of stakeholders responding to the survey**

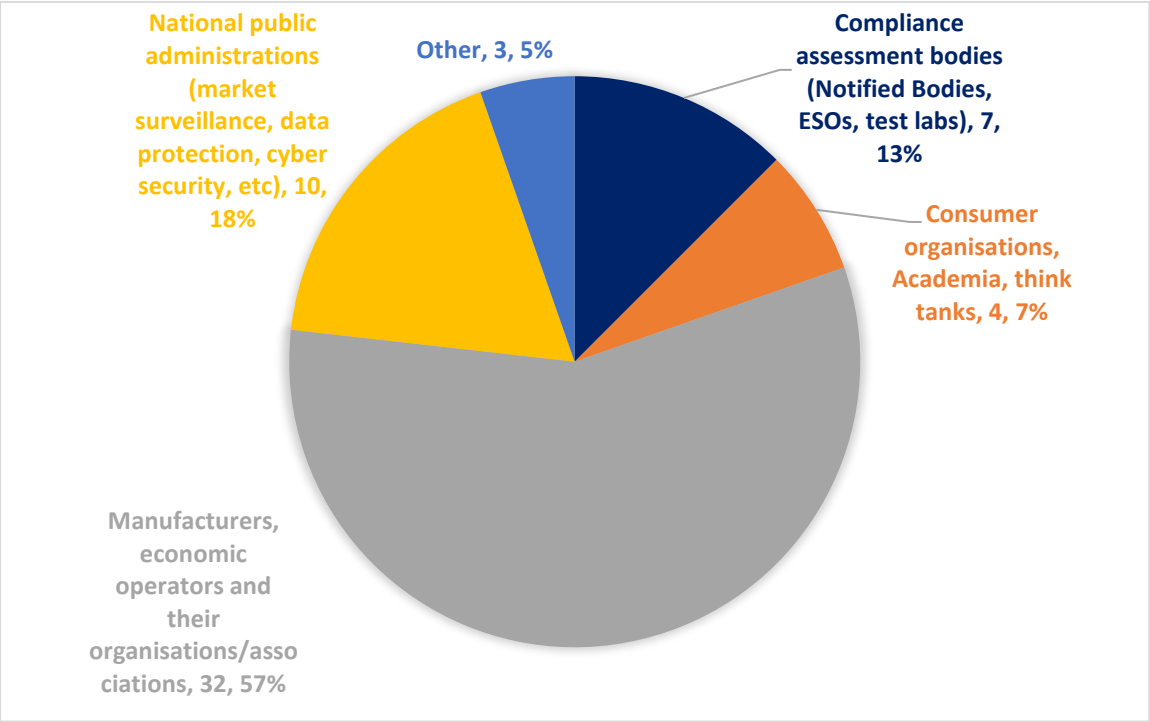
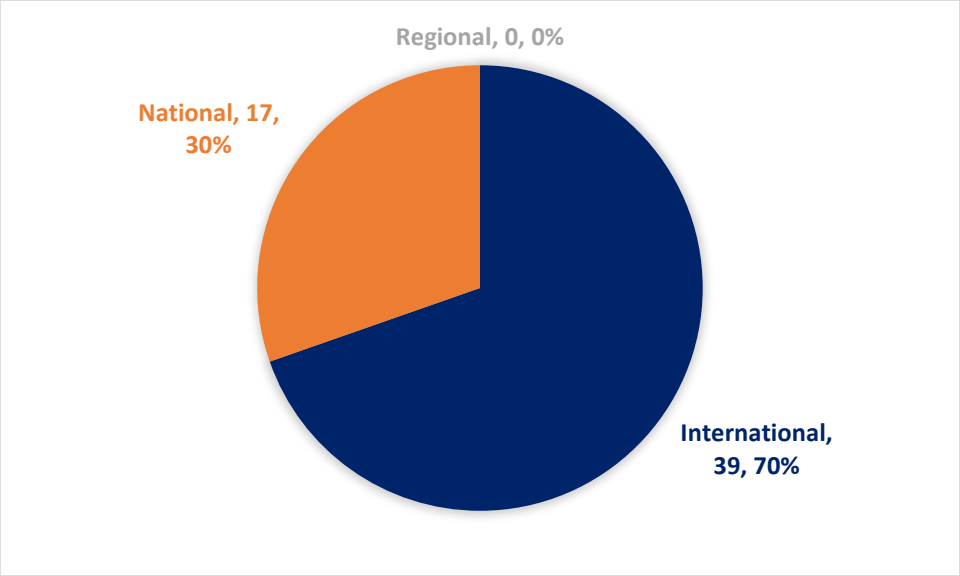



**Table 1: Number of each type of stakeholder responding to the survey**

| What kind of stakeholder is your organisation? | |
|---|---|
| Compliance assessment bodies (Notified Bodies, ESOs, test labs) | 7 |
| Consumer organisations, Academia, think tanks | 4 |
| Manufacturers, economic operators and their organisations/associations | 32 |
| National public administrations (market surveillance, data protection, cyber security, etc) | 10 |
| Technical expert (other) | 1 |
| Regulation impact Assessment Consultant (other) | 1 |
| Law firm (other) | 1 |
| **TOTAL** | **56** |

Most respondents (39) operated at the international level (including EU level), whilst the other 17 operated nationally (the 10 national public administrations plus six supply-side bodies and the one consultant).

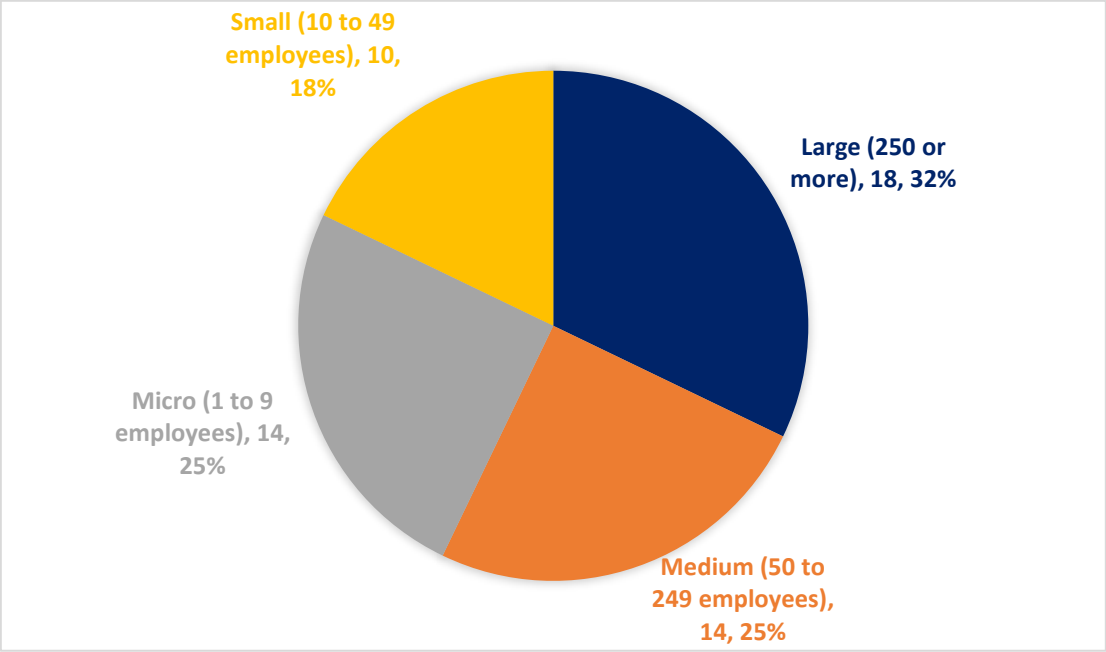
**Figure 3: Respondents' geographic scope of operations**




## 2.3 Size of organisation

There was a balance in the size of organisations responding. Large organisations were all manufacturers or national public administrations, except for two compliance assessment bodies and one university. Many of the micro-organisations were industry or consumer associations. The small and medium sized organisations were a mix of all types of organisation.

**Figure 4: Size of organisations responding to the survey**

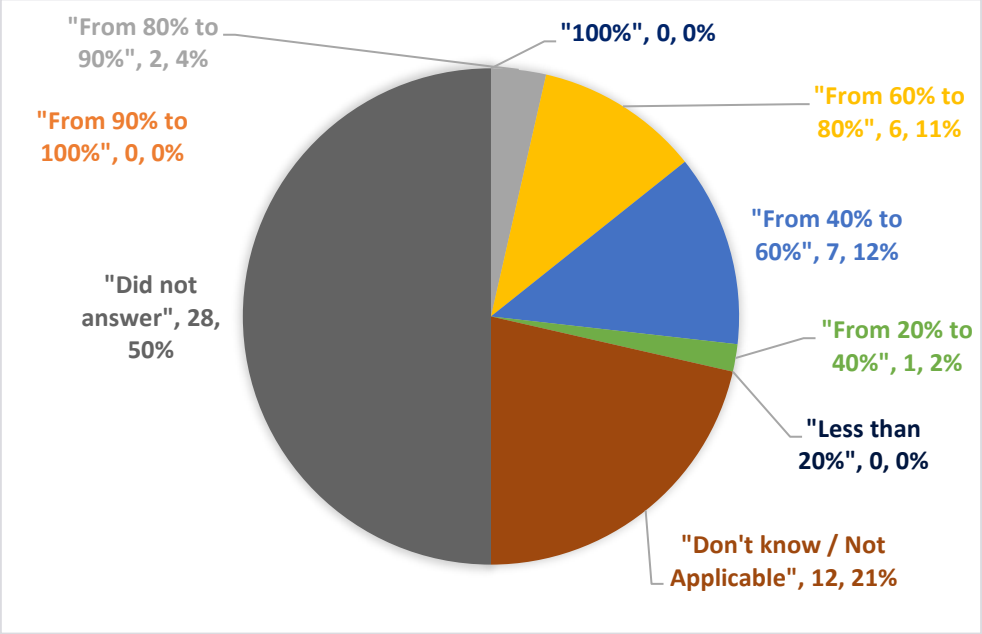


# 3. Baseline position

## 3.1 Proportion of devices affected

The RED is concerned with devices that use the radio spectrum for communication and/or radio determination purposes. This includes all internet-connected radio equipment devices. Respondents were asked to estimate the approximate percentage of wireless devices out of all internet-connected devices (including cabled or soldered equipment with a wireless connectivity, e.g. home routers).

**Figure 5: Percent of wireless devices out of all internet-connected devices**




One respondent suggested that the percentage of wireless devices amongst all internet connected devices has been estimated at 40-60% by the Ericsson Annual Mobility Report (2018).[2]

## 3.2 Current approaches to ensuring data protection by design and default

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 (12 out of 22) used international standards, whilst the rest (9 out of 22) used internal procedures and one said that it varied amongst their members.

[2] CSES was not able to confirm the validity of this reference.

**Table 2: How respondents (or the majority of their affiliates) ensure "data protection by design & default" requested by certain EU laws (e.g. the GDPR) in the products that they place on the EU market?**

| Mechanism used | Number of respondents |
|---|---|
| Through international standards | 12 |
| Through EU/EEA/EFTA standards | 0 |
| Through national/regional standards of an EU/EEA/EFTA Country | 0 |
| Through standards from non-EU/EEA Country | 0 |
| Through an internal procedure | 9 |
| Through a third-party certification | 0 |
| Other | 1 |
| Don't know / not applicable | 5 |
| Did not answer | 29 |
| **TOTAL** | **56** |

When asked to specify, respondents referred to the following standards used to ensure compliance:

- ISO/IEC 27000 series3, 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:

- Harmonised standards listed in the OJEU providing presumption of conformity are key.
- 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.

## 3.3 Adequacy of current legal framework

Currently there are no legal requirements regarding (i) data protection and privacy and (ii) protection from fraud that wireless connected devices and wearable devices have to fulfil as a condition for market access. There are however wider regulatory requirements that are applicable to any personal

[3] The ISO/IEC 27000-series (also known as the 'ISMS Family of Standards' or 'ISO27K' for short) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

data being collected by processors, such as Art. 25 GDPR (data protection by design and default). Stakeholders were therefore asked about the extent to which the lack of a mandatory legal requirement in these areas within the RED itself constituted a problem.

As the next two charts show, around three-quarters of respondents felt that the lack of a mandatory legal requirement constituted problems around both data protection and privacy, and protection from fraud. However, there were differing views about the scale of the problem, with around one quarter of all respondents believing that the risks to data protection and privacy were only minor (27%) and believing that the risks to protection from fraud were only minor (24%).

**Figure 6: Data privacy and protection risk resulting from lack of legal requirements**

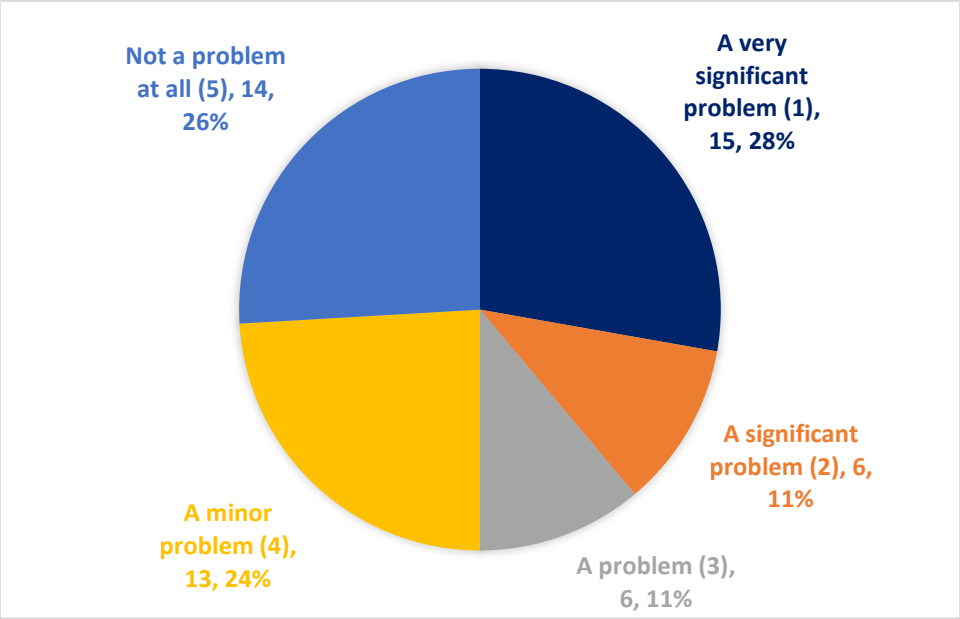
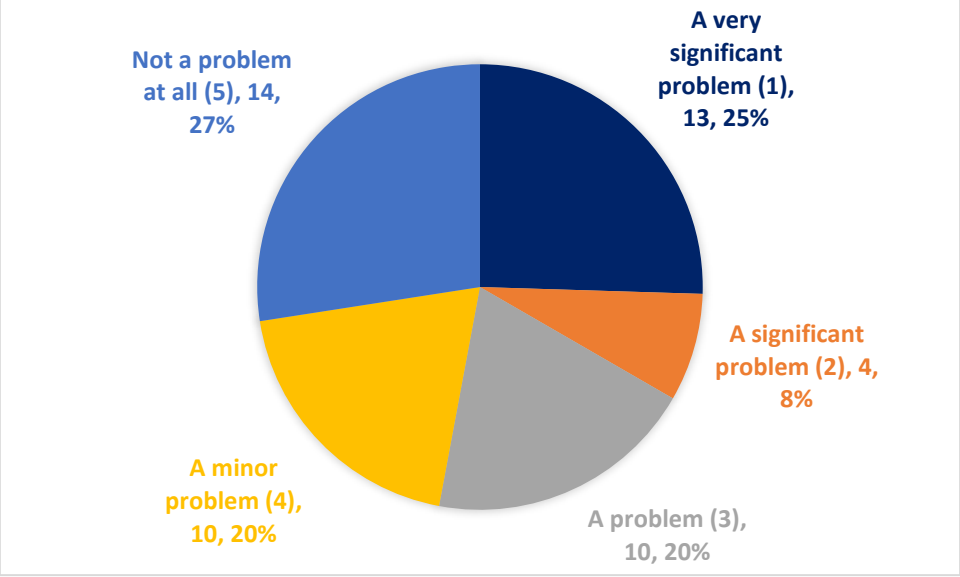
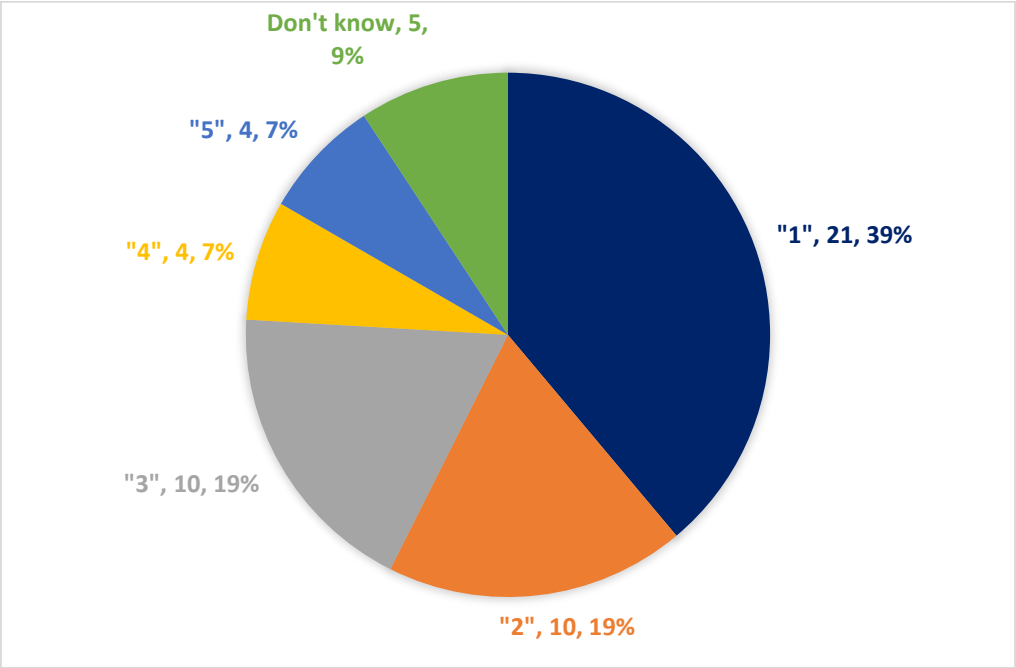



**Figure 7: Fraud risk resulting from lack of legal requirements**



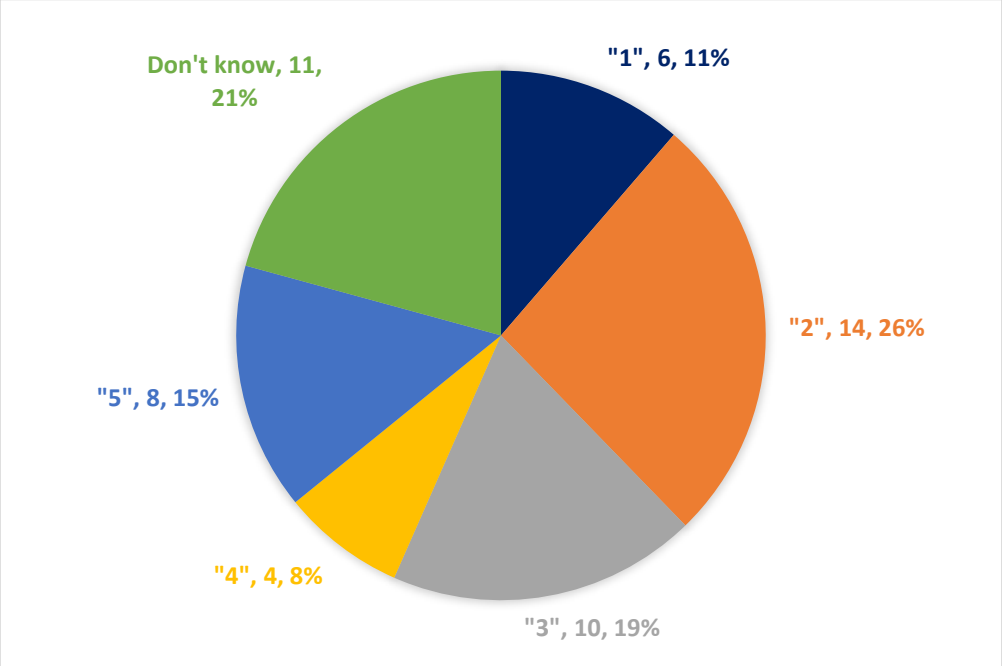

Respondents were asked whether other EU legislation (e.g. GDPR, e-Privacy Directive, cybersecurity certification through the Cybersecurity Act) provides sufficient protection in respect of i) data and privacy protection; and ii) protection from fraud.

**Figure 8: Extent to which respondents believed adequate safeguards are in place for data protection and privacy (including through existing EU legislation)**




*1 = "agree strongly", 5 = "disagree strongly"*

**Figure 9: Extent to which respondents believed adequate safeguards are in place for protection from fraud (including through existing EU legislation)**




*1 = "agree strongly", 5 = "disagree strongly"*

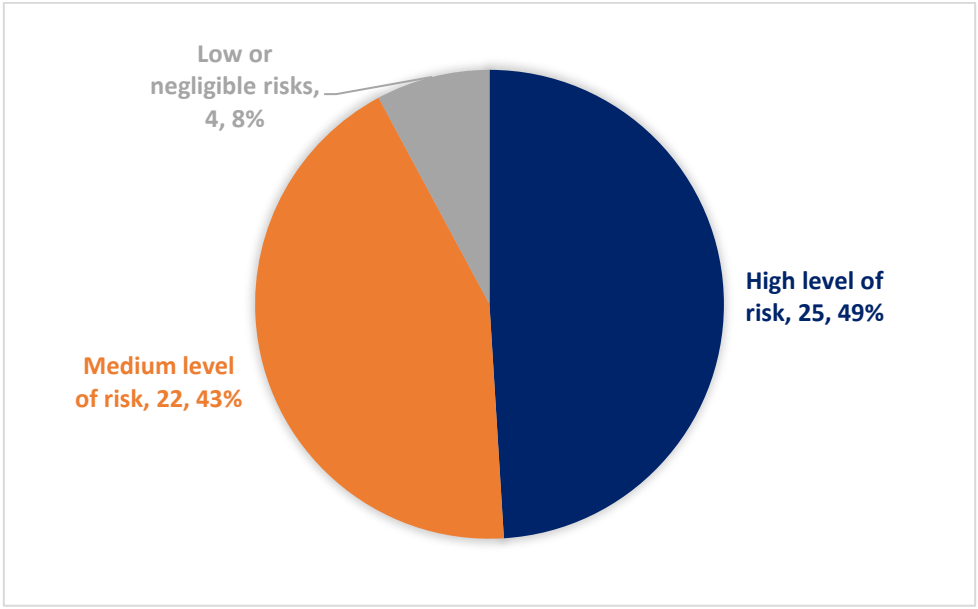
Several respondents expressed the view that, since most of the risks are common to other products outside the scope of the RED, the most appropriate way to address them would be through horizontal legislation, such as the General Data Protection Regulation (GDPR)[4] or the (currently voluntary) Cybersecurity Act (CSA).[5] This suggestion also emerged in response to questions related to the level of support for new regulatory requirements (see section 4.3 below).

## 3.4 Extent of risks relating to wireless connected devices

Respondents to the targeted consultation were then asked for their views about the extent to which there are risks relating to wireless connected devices.

As the four charts below show, there is a strong consensus that wireless connected and wearable devices are associated with risks related to data protection and privacy, and protection from fraud, with only a small minority of respondents believing that the risks are low or negligible.

**Figure 10: Data and privacy protection risk related to wireless connected devices**




[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

**Figure 11: Data and privacy protection risk related to wearable devices**

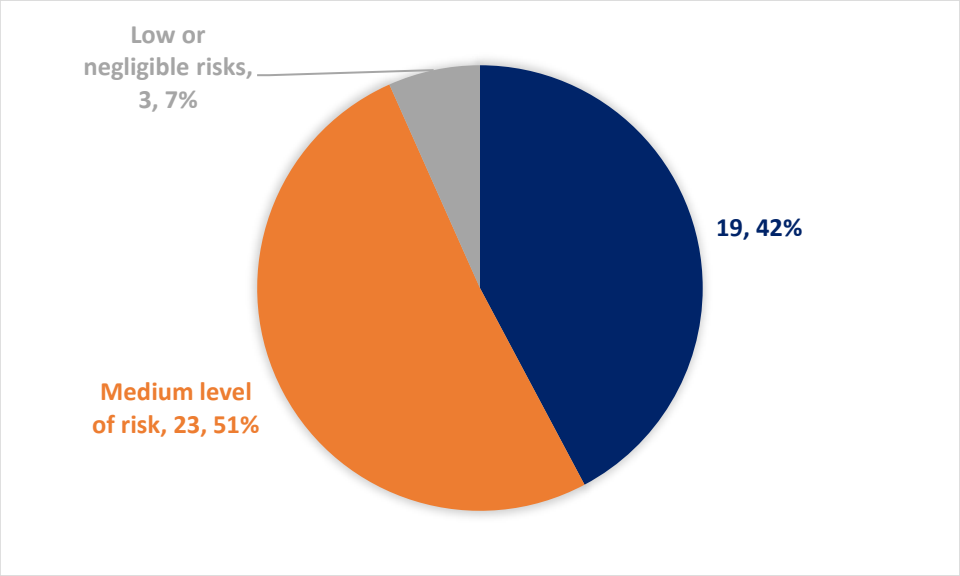



**Figure 12: Fraud risk related to wireless connected devices**

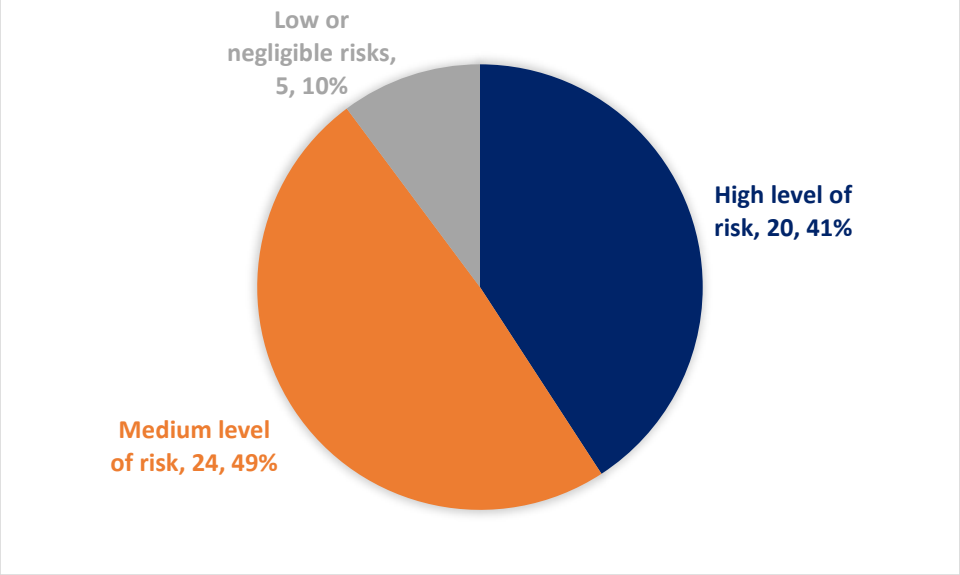
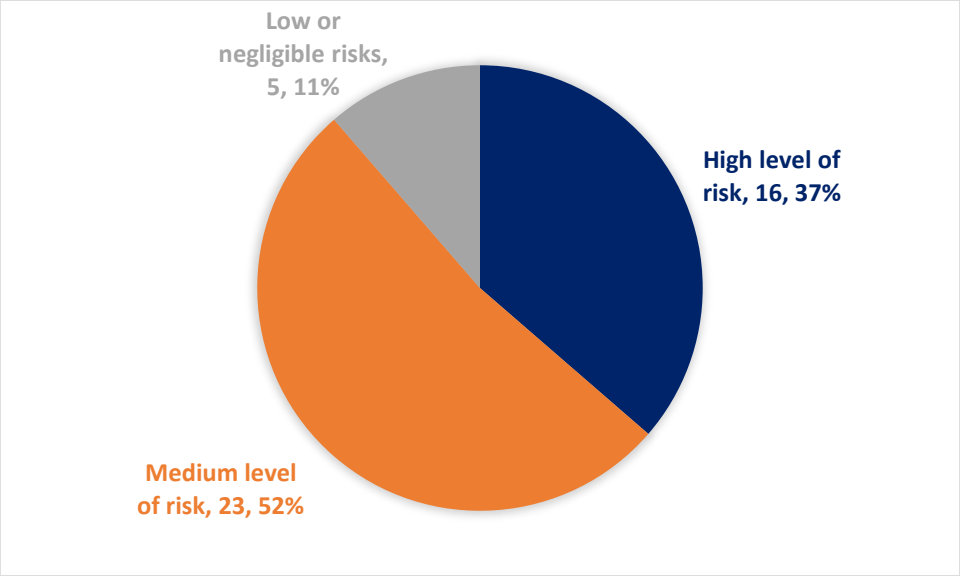


**Figure 13: Fraud risk related to wearable devices**




The responses to the open questions provided some insights into stakeholders' views. They showed some consensus over the existence and nature of risks related to internet-connected radio equipment devices and wearables, but differing views over the origin of such risks and the best way to address them.

Of those offering comments, the stakeholders were virtually unanimous in stating the view that connected **wireless devices create real risks to data and privacy protection and protection from fraud** that need to be addressed by EU legislation. As one stated, "without an adequate regulatory framework, IoT devices will remain vulnerable to, in particular, hacking, manipulation and theft of data". Two respondents offering identical responses stated that "data protection from fraud is an issue for all connected devices". Another referenced research undertaken by the European Union Agency for Cybersecurity (ENISA) and the US government (NIST) that highlighted the risks posed by insecure internet-connected devices. Just one respondent, a large manufacturer, reported that it did not see a problem with the current situation; however, the respondent did not clarify whether this was because the devices did not raise risks or because the current legal framework (e.g. GDPR Art. 25) is adequate to address any risks.

One consumer body also identified an additional risk, i.e. that of a collective attack ("botnet") using unsecured IoT devices which may cause a degradation of service or be used to attack particular websites or even critical infrastructures. It suggested the adoption of a delegated act under Article 3(3)d, i.e. relating to radio equipment harming networks and causing degradation of service. Whilst outside the formal scope of this study, which focuses on Article 3(3)e and Article 3(3)f, it is nevertheless worth mentioning that the inter-connection between these three articles and the risk of botnet attacks using IoT devices was also mentioned by several interviewees.

There was a **divergence of opinion regarding the origin of any risk.** Several respondents suggested that there was an inherent problem with the way that devices are designed, manufactured and sold. One large manufacturer (based outside the EU) stated that, for some manufacturers, "cybersecurity is often an afterthought." Another respondent stated that "the security of IoT devices is poor, they are produced at mass scale at low cost with many devices from outside the EU". Another reported that devices can be hacked quickly, linked to problems of shadow usage, lack of timely software and firmware updates, patches and backdoors. One respondent suggested that vendors did not care sufficiently about data security. One consumer organisation referred to tests that have shown that

certain connected products placed on the market come with multiple security risks and flaws. Some respondents highlighted that any risks associated with products were aggravated by a lack of awareness or interest on the part of users who "do not know and do not care".

In contrast, several respondents suggested that **the problem is not with the devices themselves but with the service providers**, i.e. it is a problem of transfer and downstream processing of data. For example, one reported that the problem lay with communication services, cloud services, networks and (all) network products, which all contribute to risks to data and privacy protection and protection from fraud. This is interesting in that data processing is regulated by the GDPR, and the transmission of data via electronic communications by the e-Privacy Directive. However, the current legal framework still seems to be inadequate to address concerns regarding data security.

Several respondents also pointed out that **the problem is not limited to wireless connected devices**, but also affects wired devices. As a result, those respondents mostly considered that the use of delegated acts under the RED was not the most appropriate solution to the problem. An alternative raised was the possibility of introducing a horizontal mandatory piece of legislation covering all types of products. This would cover minimum baseline requirements in cybersecurity to help ensure adequate safeguards for data protection and privacy and protection from fraud.

## 3.5 Risks associated with specific types of devices

Respondents were asked to rate the extent of risks with respect to data and privacy protection, relating to specific subcategories of products. More than 85% of respondents (and more than 90% in most cases) believed that there was a medium or high level of risk associated with these products, as shown by the chart below.

**Figure 14: Level of risk associated with different types of device (data and privacy)**

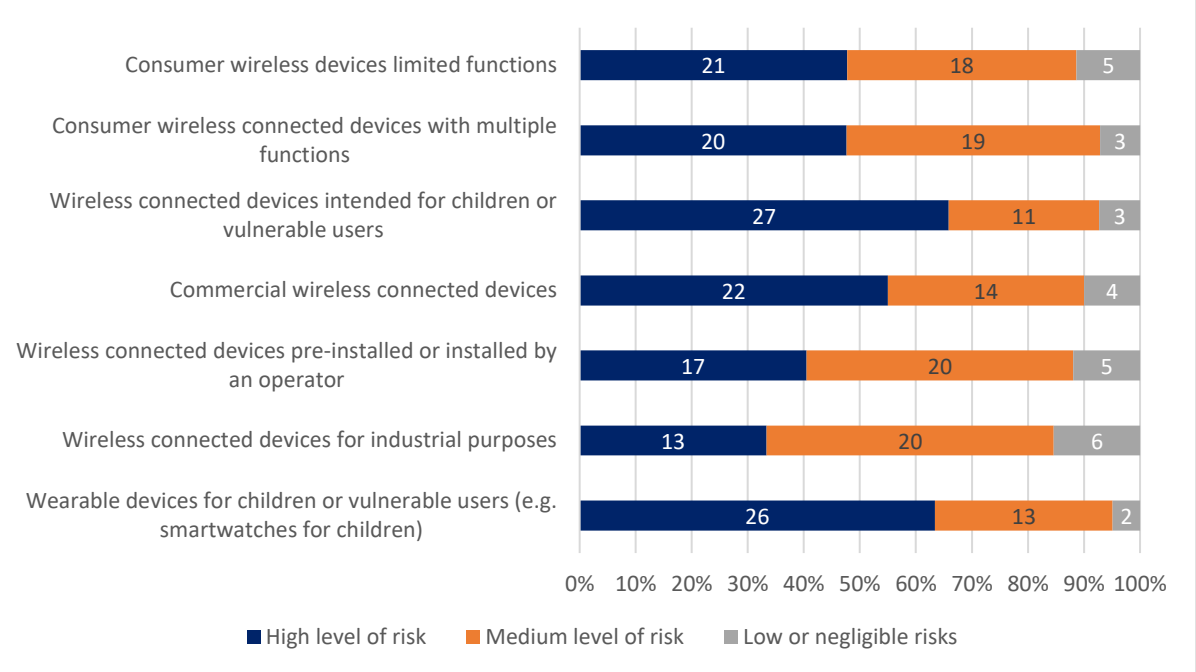


**Table 3: Number of respondents reporting risks from different types of device (data and privacy)**

| Connected Devices | High level of risk (#) | Medium level of risk (#) | Low or negligible risks (#) | Don't know | Did not answer |
|---|---|---|---|---|---|
| Consumer wireless devices limited functions | 48% | 41% | 11% | 1 | 11 |
| Consumer wireless connected devices with multiple functions | 48% | 45% | 7% | 2 | 12 |
| Wireless connected devices intended for children or vulnerable users | 66% | 27% | 7% | 3 | 12 |
| Commercial wireless connected devices | 55% | 35% | 10% | 4 | 12 |
| Wireless connected devices pre-installed or installed by an operator | 40% | 48% | 12% | 2 | 12 |
| Wireless connected devices for industrial purposes | 33% | 51% | 15% | 5 | 12 |
| Wearable devices for children or vulnerable users (e.g. smartwatches for children) | 63% | 32% | 5% | 3 | 12 |

With respect to protection from fraud, more than 80% of respondents (and more than 85% in most cases) believed that there was a medium or high level of risk associated with these products, as shown by the chart below.

**Figure 15: Level of risk associated with different types of device (fraud)**

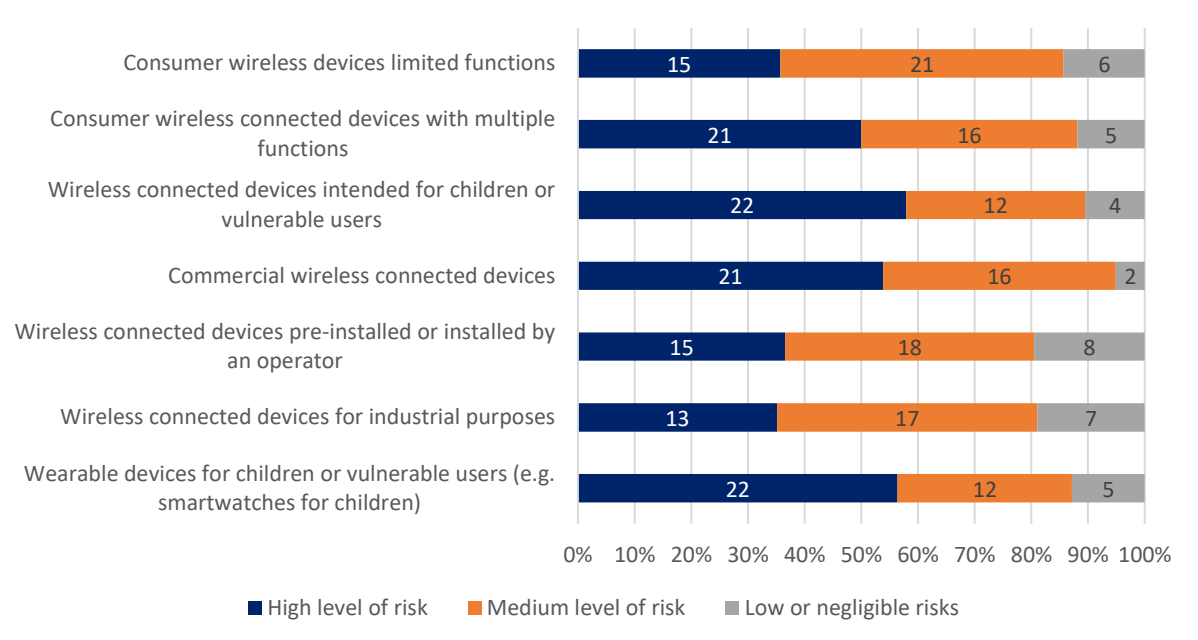


**Table 4: Number of respondents reporting risks from different types of device (fraud)**

| Connected Devices | High level of risk (%) | Medium level of risk (%) | Low or negligible risks (%) | Don't know | Did not answer |
|---|---|---|---|---|---|
| Consumer wireless devices limited functions | 36% | 50% | 14% | 2 | 12 |
| Consumer wireless connected devices with multiple functions | 50% | 38% | 12% | 2 | 12 |
| Wireless connected devices intended for children / vulnerable users | 58% | 32% | 11% | 6 | 12 |
| Commercial wireless connected devices | 54% | 41% | 5% | 5 | 12 |
| Wireless connected devices pre-installed or installed by an operator | 37% | 44% | 20% | 3 | 12 |
| Wireless connected devices for industrial purposes | 35% | 46% | 19% | 7 | 12 |
| Wearable devices for children or vulnerable users (e.g. smartwatches for children) | 56% | 31% | 13% | 5 | 12 |

When asked to comment on the specific risks related to these different subcategories of products, stakeholders offered few comments. Instead, they mostly commented on the risks affecting wireless products in general (or products with both wireless and wired functionality) or on possible solutions for all types of products. The comments about the specific subcategories of products were as follows:

- **Consumer devices with limited functions**: the representative of a national government reported that the risks of fraud related to devices with limited or multiple functions were generally high depending on the type of application (e.g. greater in devices with authentication of payment functions). In contrast, a European trade association suggested that home appliances were generally low risk (although its members' products perhaps tend not to include functions associated with higher-levels of risk, e.g. kitchen appliances, toothbrushes, air conditioners).
- **Consumer devices with multiple functions**: one respondent reported that devices with multiple functions may give more possibilities for security measures by the end-user than devices with limited functions, but their risks may be larger due to their greater complexity and larger attack surface.
- **Devices intended for children or vulnerable users**: one stakeholder suggested that there were no risks related specifically to such devices, only the general risk that a product processes sensitive data. The stakeholder pointed out the same (high) level of security would need to apply to any consumer device, since many devices are used autonomously by children whilst not being designed for them. One consumer organisation referred to tests showing that with a few simple steps, anyone could access the microphone of a certain type of connected toy and speak with the children without the knowledge of their parents.
- **Commercial devices**: two respondents highlighted that the security of public Wi-Fi was generally

low and one highlighted risks associated with point of sales terminals and vending machines. One European industry body suggested that commercial devices entail a higher risk level than consumer devices.

- **Devices pre-installed or installed by an operator**: no comments were offered.
- **Industrial devices**: one respondent suggested that risks might result from a neglect of cyber security considerations in relation to operational technology security. Another stated that risks could be reduced where the end-user can take mitigating measures in a managed system. Another suggested that safety of industrial applications is usually ensured by contractual agreements and are thus low.
- **Wearable devices for children or vulnerable users**: Tests on a smart watches also showed that a third-party could easily change the geo-location of the watch ('location spoofing') as well as track and contact the user directly. Whilst this would affect any user, it would clearly raise particular risks in relation to children and other vulnerable users.

## 3.6 Specific risks to users

Respondents were also asked about the extent to which they were concerned about specific types of risk for users of wireless connected devices and wearable devices. However, only 4 out of 56 stakeholders offered a response to this question and these responses were divergent:

- Two consumer organisations reported a high level of concern (1/5) for all of these risks.
- One university had a high level of concern about "data being recorded on an unauthorised basis" and "unauthorised transfer or processing of data for marketing or other purposes" and fairly high concern (2/5) about "general adequacy of data protection built into the connected equipment" and about "geolocational data of the user".
- One research institute had low concerns about all risks, except for "geolocational data of the user", which it rated as a medium (3/5).

The two consumer organisations also highlighted two other risks:

- Insecure connected products risk being used as part of a collective attack ("botnet"), the purpose of which is to cause a degradation of a service.
- Damaging or destroying ("bricking") connected equipment as a result of hacking and/or malware.

**Table 5: Number of respondents with concerns about specific risks**

| Level of concern (1= high; 5 = low) | 1 | 2 | 3 | 4 | 5 | Did not answer |
|---|---|---|---|---|---|---|
| General adequacy of data protection built into the connected equipment | 2 | 1 | 0 | 0 | 1 | 52 |
| General adequacy of protection from fraud in wearables and other types of radio equipment | 2 | 0 | 1 | 0 | 1 | 52 |
| Geolocational data of the user | 2 | 1 | 1 | 0 | 0 | 52 |
| Data being recorded on an unauthorised basis | 3 | 0 | 0 | 0 | 1 | 52 |
| Unauthorised transfer or processing of data for marketing or other purposes | 3 | 0 | 0 | 0 | 1 | 52 |
| Other risks | 2 | 0 | 0 | 0 | 0 | 54 |

## 3.7 Specific risks to children and vulnerable consumers

Respondents were also asked about the extent to which they were concerned about specific types of risk for children or vulnerable consumers when using wireless connected devices and wearable devices. The same 4 out of 56 stakeholders offered a response to this question and these responses were again divergent.

- Two consumer organisations reported a high level of concern (1/5) for all types of risks.
- The research institute had low concerns (5/5) about all risks, except for "General adequacy of protection from fraud", which it rated as fairly low (4/5).
- The university had high concern about "data being recorded on an unauthorised basis" and "unauthorised transfer of product data usage for marketing purposes" and fairly high (2/5) or medium (3/5) level of concern about all other risks.

**Table 6: Number of respondents with concerns about specific risks to children and vulnerable users**

| Level of concern (1= high; 5 = low) | 1 | 2 | 3 | 4 | 5 | Did not answer |
|---|---|---|---|---|---|---|
| General adequacy of data protection built into smart toys, wearables and other types of radio equipment | 2 | 1 | 0 | 0 | 1 | 52 |
| General adequacy of protection from fraud in smart toys, wearables and other types of radio equipment | 2 | 0 | 1 | 1 | 0 | 52 |
| Geolocational data of child being tracked or compromised | 2 | 1 | 0 | 0 | 1 | 52 |
| Third party interacting with the child / user | 2 | 1 | 0 | 0 | 1 | 52 |
| Data being recorded on an unauthorised basis (e.g. child's voice and/ or interaction with smart toy) | 3 | 0 | 0 | 0 | 1 | 52 |
| Unauthorised transfer of product data usage for marketing purposes | 3 | 0 | 0 | 0 | 1 | 52 |
| Smart toy being hacked | 2 | 0 | 1 | 0 | 1 | 52 |
| Other risks | 0 | 0 | 0 | 0 | 0 | 56 |

## 3.8 Technical possibilities to mitigate risks

The stakeholders were asked to comment on whether it was technically possible to mitigate risks related to data and privacy protection and protection from fraud. There was a strong degree of consensus on this question, with the overwhelming majority of respondents agreeing that it was possible to a great or moderate extent to mitigate such risks for all types of wireless or wearable products. There was also a strong consensus that such mitigation techniques can be progressively and proportionately applied throughout the value chain.

The open question allowed respondents to provide examples. They included the following:

- Security by design and default: including default settings that do not allow open access, forcing users to change default passwords, strong authentication mechanisms, limited communication to periods when the device is in operation, encrypted communications, options to delete personal

accounts and personal data (e.g. if disposing of the device). As one respondent suggested “default settings must always be the secure ones”. A few respondents suggested that security by design and default could be improved by the application of mandatory requirements and EU standards or by security certification schemes or security protocols in each part of the value chain.

- Ensuring that upstream devices, e.g. routers, can protect devices that are connected to the network via wireless internet access. A few respondents highlighted that most consumer radio equipment products are only indirectly connected to the internet via routers or switches. It would therefore be sufficient to ensure that such upstream devices are secure.
- Security updates post-sale: including distribution of patches and forced updates, in order to adapt to new or changing threats.
- Market surveillance: for example, to check application of risk-mitigation principles.
- Raising user awareness of risks and how to mitigate them.

**Figure 16: Technical possibility of mitigating risk**

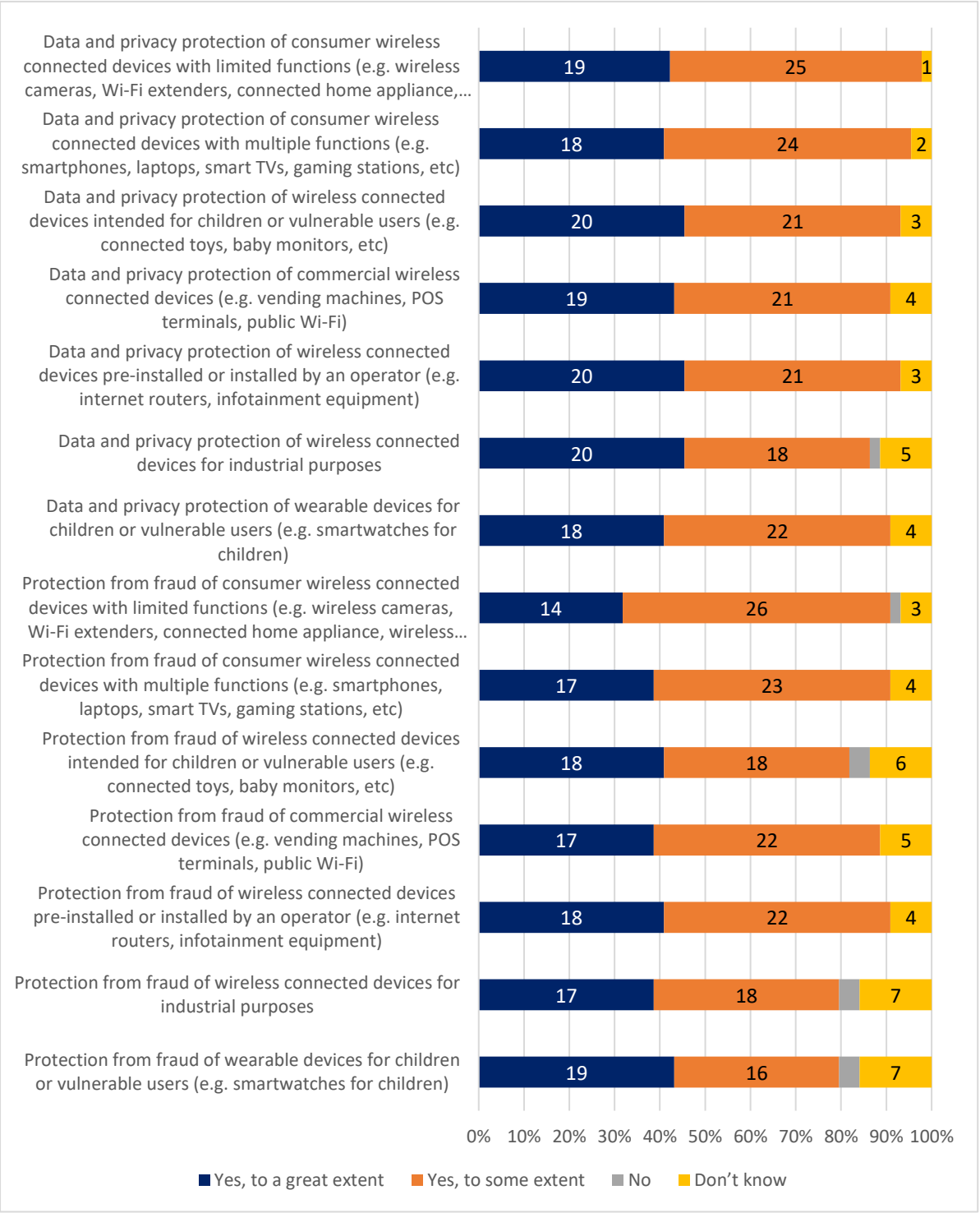


**Table 7: Technical possibility of mitigating risk**

| Risks | Yes, to a great extent | Yes, to some extent | No | Don't know |
|---|---|---|---|---|
| Data and privacy protection of consumer wireless connected devices with limited functions (e.g. wireless cameras, Wi-Fi extenders, connected home appliance, wireless thermostats, etc) | 42% | 56% | 0% | 2% |
| Data and privacy protection of consumer wireless connected devices with multiple functions (e.g. smartphones, laptops, smart TVs, gaming stations, etc) | 41% | 55% | 0% | 5% |
| Data and privacy protection of wireless connected devices intended for children or vulnerable users (e.g. connected toys, baby monitors, etc) | 45% | 48% | 0% | 7% |
| Data and privacy protection of commercial wireless connected devices (e.g. vending machines, POS terminals, public Wi-Fi) | 43% | 48% | 0% | 9% |
| Data and privacy protection of wireless connected devices pre-installed or installed by an operator (e.g. internet routers, infotainment equipment) | 45% | 48% | 0% | 7% |
| Data and privacy protection of wireless connected devices for industrial purposes | 45% | 41% | 2% | 11% |
| Data and privacy protection of wearable devices for children or vulnerable users (e.g. smartwatches for children) | 41% | 50% | 0% | 9% |
| Protection from fraud of consumer wireless connected devices with limited functions (e.g. wireless cameras, Wi-Fi extenders, connected home appliance, wireless thermostats, etc) | 32% | 59% | 2% | 7% |
| Protection from fraud of consumer wireless connected devices with multiple functions (e.g. smartphones, laptops, smart TVs, gaming stations, etc) | 39% | 52% | 0% | 9% |
| Protection from fraud of wireless connected devices intended for children or vulnerable users (e.g. connected toys, baby monitors, etc) | 41% | 41% | 5% | 14% |
| Protection from fraud of commercial wireless connected devices (e.g. vending machines, POS terminal, public Wi-Fi) | 39% | 50% | 0% | 11% |
| Protection from fraud of wireless connected devices pre-installed or installed by an operator (e.g. internet routers, infotainment equipment) | 41% | 50% | 0% | 9% |
| Protection from fraud of wireless connected devices for industrial purposes | 39% | 41% | 5% | 16% |
| Protection from fraud of wearable devices for children or vulnerable users (e.g. smartwatches for children) | 43% | 36% | 5% | 16% |

# 4. Policy options

## 4.1 Overview of options

The consultation explored a range of questions regarding different options for revision of the RED:

- **Option 0 - baseline scenario**: a situation in which manufacturers are not obliged to implement any specific measures, as is currently the case.
- **Option 1 – industry self-regulation**: a situation whereby the **industry self-regulates** to implement the existing legislation which protects personal data, the confidentiality of telecommunications, security and protection against fraud.
- **Option 2 - regulatory requirement on data and privacy**: adoption of a delegated act pursuant to Article 3(3)(e). This will require that radio equipment incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected, also as a tool to enhance the cybersecurity of these products, and this requirement will have to be demonstrated for the purposes of market access.
- **Option 3 - regulatory requirement on protection from fraud**: adoption of a delegated act pursuant to Article 3(3)(f). This will require that radio equipment incorporates certain features ensuring protection from fraud, also as a tool to enhance the cybersecurity of these products, and this requirement will have to be demonstrated for the purposes of market access.
- **Option 4: regulatory requirement on data and privacy and protection from fraud**: adoption of a delegated act pursuant both Articles 3(3) (e) and (f). In this case, both requirements in Options 2 and 3 will have to be demonstrated for the purposes of market access.

A small number of stakeholders alluded to a further regulatory option, that of a possible horizontal piece of legislation on ensuring basic minimum cybersecurity functionality of all connected industrial products, irrespective of whether these are wireless (and integrate radio functionality) or are wired.

## 4.2 Level of support for self-regulation

Respondents were asked to compare the effectiveness and viability of a voluntary or self-regulatory approach with a regulatory approach. As shown in Figure 17 and Table 8 below, there was a divergence of views with just less than half of respondents believing that a voluntary or self-regulatory approach was less effective than a regulatory approach and just over half believing that it was as effective or more effective.

The divergence of views was explained by the type of stakeholder responding. For example, in respect of a self-regulatory approach, those believing it was:

- Less effective (22) were mostly compliance assessment bodies, national public administrations, consumer organisations and other (e.g. law firm); only five were economic operators;
- More or equally effective (27) were mostly economic operators (21), the others being compliance assessment bodies (4), national public administrations (2).

The divergence of views by type of stakeholder was also evident in responses concerning the viability of a self-regulatory or voluntary approach, as shown in Figure 18 and Table 9.

Several manufacturers suggested that voluntary or self-regulatory approaches would be more appropriate, as they can adapt to the changing environment and new threats more easily. One suggested that a voluntary certification scheme could be developed, which might then become

mandatory at a later date, depending on its effectiveness, as had been done under the Cybersecurity Act. Another respondent, an association representing more than 500 member companies, pointed to its own certification scheme, which aims to ensures security by design.

**Figure 17: Relative effectiveness of different approaches to regulation (Self-regulatory/voluntary approach compared to a regulatory approach)**

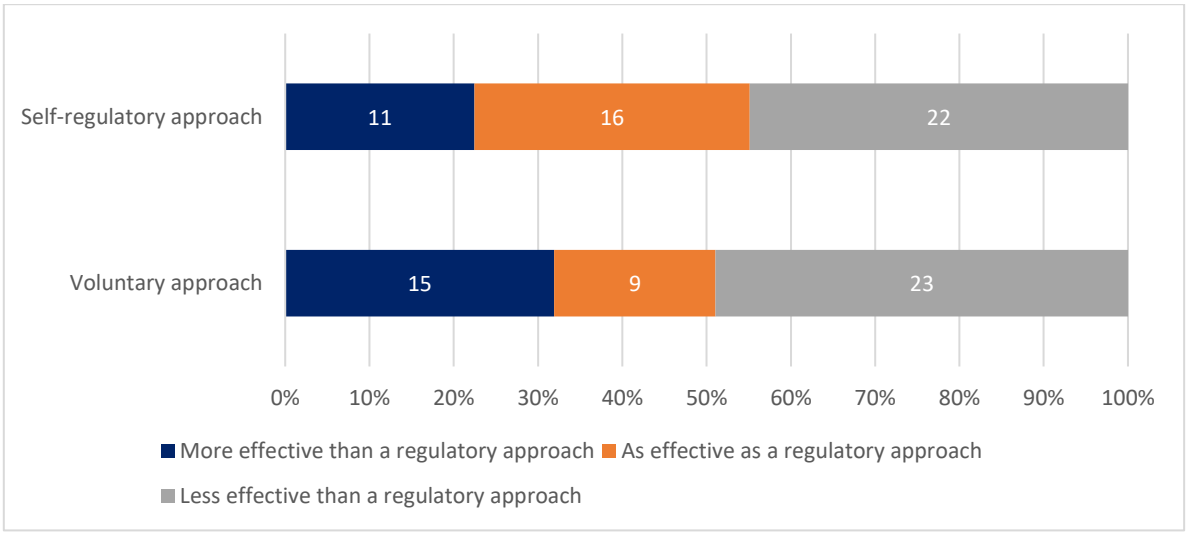



**Table 8: Relative effectiveness of different approaches to regulation**

| Type of approach | More effective than a regulatory approach | As effective as a regulatory approach | Less effective than a regulatory approach |
|---|---|---|---|
| Self-regulatory approach | 22% | 33% | 45% |
| Voluntary approach | 32% | 19% | 49% |

**Figure 18: Relative viability of different approaches to regulation (Viability of a self-regulatory approach/voluntary approach compared to a regulatory approach)**

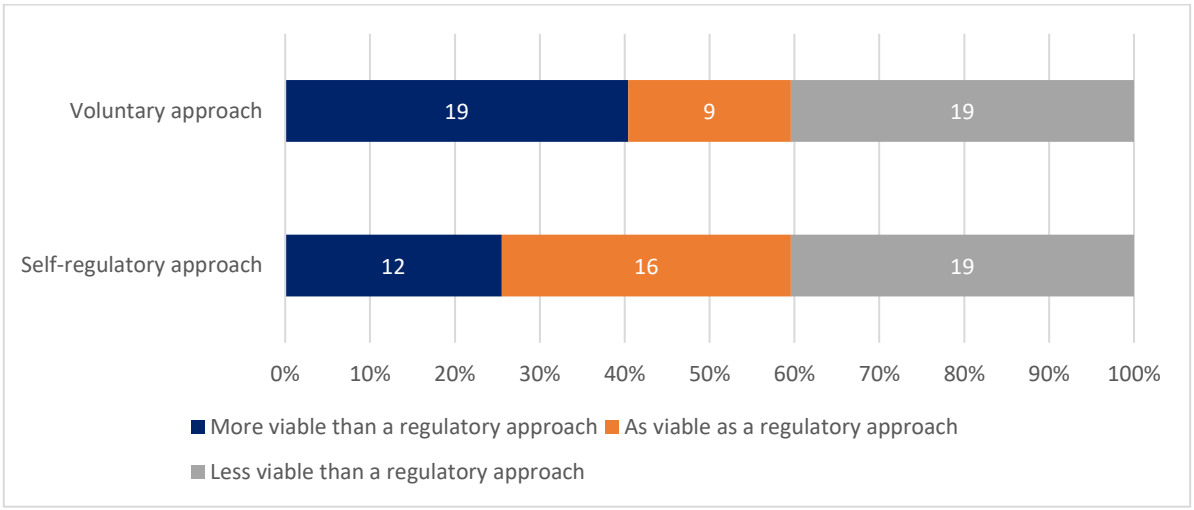


**Table 9: Relative viability of different approaches to regulation**

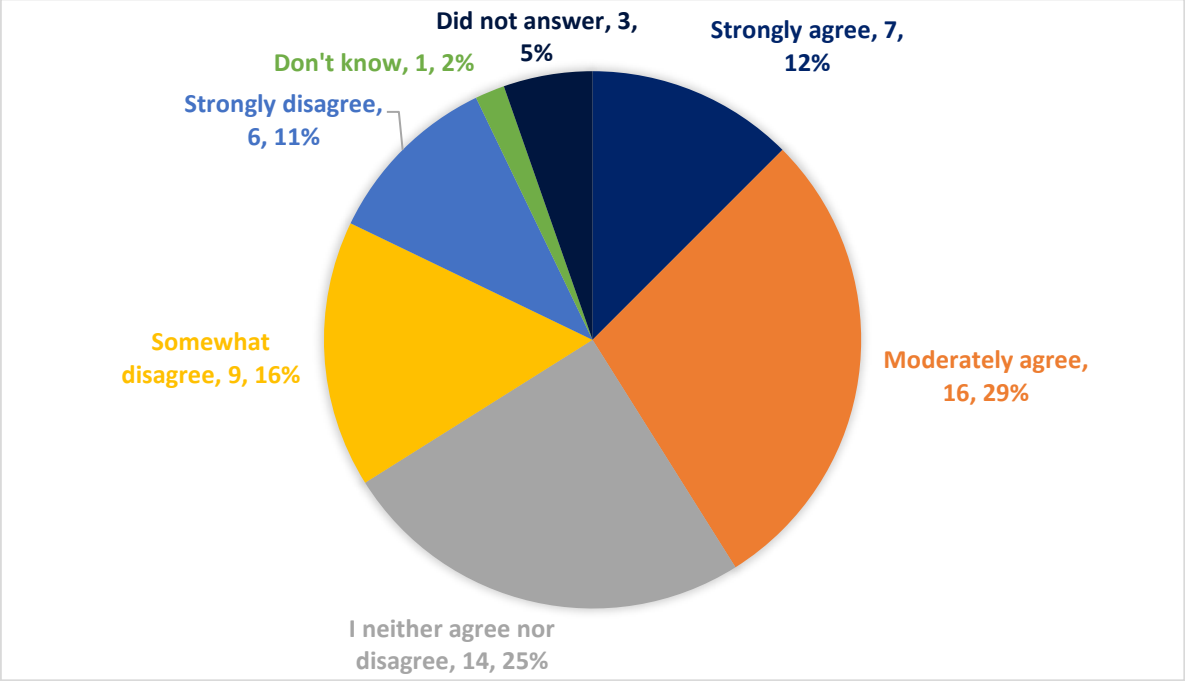
| Type of approach | More viable than a regulatory approach | As viable as a regulatory approach | Less viable than a regulatory approach |
|---|---|---|---|
| Self-regulatory approach | 40% | 19% | 40% |
| Voluntary approach | 26% | 34% | 40% |

The same divergence of views emerged in respect of the complementarity of a voluntary or self-regulatory approach to a regulatory approach. Some 41% agreed on such complementarity, whilst 27% disagreed and 25% neither agreed nor disagreed.

Again, the divergence of views arose amongst different types of stakeholder:

- Of the 15 who disagreed, most (11) were economic operators;
- Of those who agreed, only 6 were economic operators.

**Figure 19: Complementarity of a voluntary/self-regulatory approach to a regulatory approach**




When asked to comment on their response, the respondents offered divergent views.

- Several expressed the view that delegated acts under the RED would potentially overlap or conflict with other EU legislation, such as the GDPR or the CSA. Since most of the risks are common to other products outside the scope of the RED, the suggestion was that horizontal legislation remained the most appropriate way to address them. One also suggested that any requirements should be aligned with international cybersecurity standards.
- Several respondents suggested that a (voluntary) certification scheme could be beneficial, such as one operating under the scope of the CSA.
- Several respondents highlighted the risk that some producers would only comply with regulatory requirements and not with voluntary requirements. However, one suggested that a voluntary approach might be beneficial for complex devices that are outside the scope of the RED.

- Two respondents suggested that self-regulatory and regulatory approaches would risk being ineffective, as they would divert producers' attention away from addressing actual risks and towards ensuring compliance with voluntary certification schemes, such as the CSA.

## 4.3 Level of support for new regulatory requirements

Respondents were asked whether they supported new regulatory requirements in the form or delegated acts under Articles 3(3)(e) and (f) of the RED. As shown by the figures below, there was a divergence of views with about half of respondents believing that delegated acts should be introduced and half believing they should not.

Responses to this question reflected the type of stakeholder:

- Those in favour of the delegated acts were mostly compliance assessment bodies, national public administrations, consumer organisations (e.g. law firm); only four were economic operators;
- Those against the activation of the delegated acts: were all economic operators.

**Figure 20: Support for new regulatory requirements**

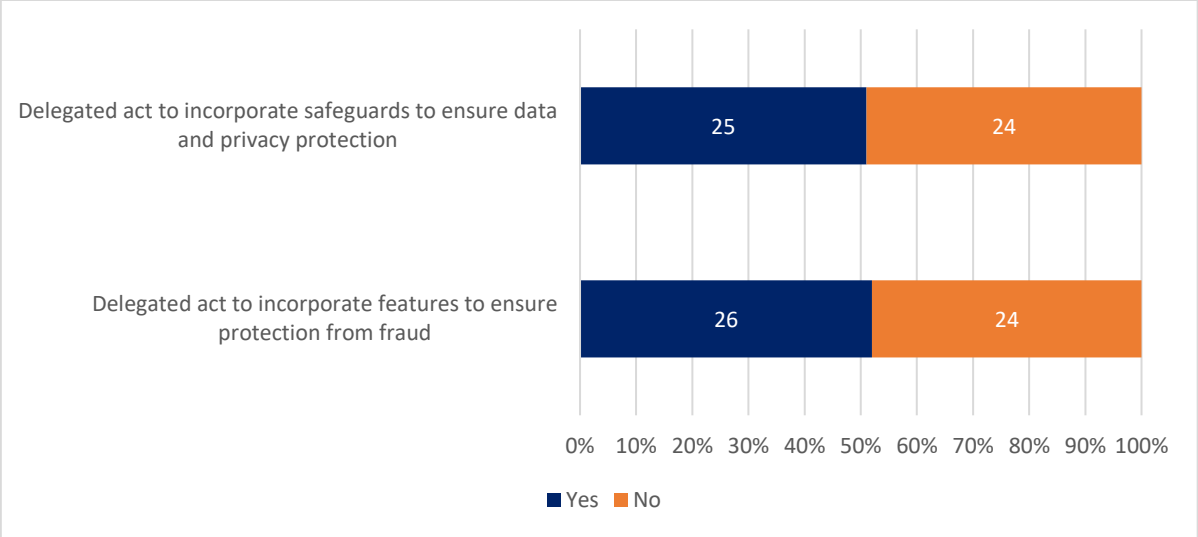



**Table 10: Support for new regulatory requirements**

| Legal requirements | Yes | No | Don't know | Did not answer |
|---|---|---|---|---|
| Delegated act to incorporate safeguards to ensure data and privacy protection | 25 | 24 | 4 | 3 |
| Delegated act to incorporate features to ensure protection from fraud | 26 | 24 | 2 | 4 |

Responses to open questions provided some insights into the views of economic operators.

Several respondents did not consider that the use of delegated acts under the RED was the most appropriate solution because **the problem is not limited to wireless connected devices**, but also affects wired devices. In their view, such a "vertical" approach would risk overlapping with other EU legislation and thus create legal uncertainty, inconsistency, etc. Instead, they suggested that data

security should be addressed by "horizontal legislation" covering all relevant products, some of which is already in place, such as the GDPR, Cybersecurity Act, Sale of Goods Directive, Digital Content Directive, e-Privacy Directive. For example, one respondent suggested that the work programme for cyber security certification being developed in relation to the Cybersecurity Act would encompass all IoT devices, including those under RED.

One respondent, a medium-sized manufacturer outside the EU, suggested that the imposition of **mandatory requirements in this area might actually aggravate the problem**. In the view of this manufacturer, a first risk was that manufacturers' effort would be directed towards ensuring compliance with such requirements instead of addressing security risks. A second risk was that a one size fits all approach might not work as devices may have different vulnerabilities, requiring the development of many different harmonised technical standards.

## 4.4 Preferred form of standards

Respondents were asked to indicate how they would prefer that an adequate level of protection concerning (i) data protection and privacy and (ii) protection from fraud would be demonstrated if future voluntary or regulatory requirements were to be adopted.

In response, the stakeholders offered a diversity of opinions. "Future harmonised standards" was the most popular approach, albeit supported only by a minority of respondents. "National or EU standards" that are already available was the least popular approach, possibly as these would need to be translated into harmonised technical standards before they could be useful in demonstrating compliance with the essential requirements.

When asked to specify "other ways to ensure an adequate level of protection", several stakeholders restated the view that protection should be ensured by baseline requirements under horizonal EU legislation covering all products on the market, not just those covered by the RED.

**Figure 21: Preferred standards under delegated acts**

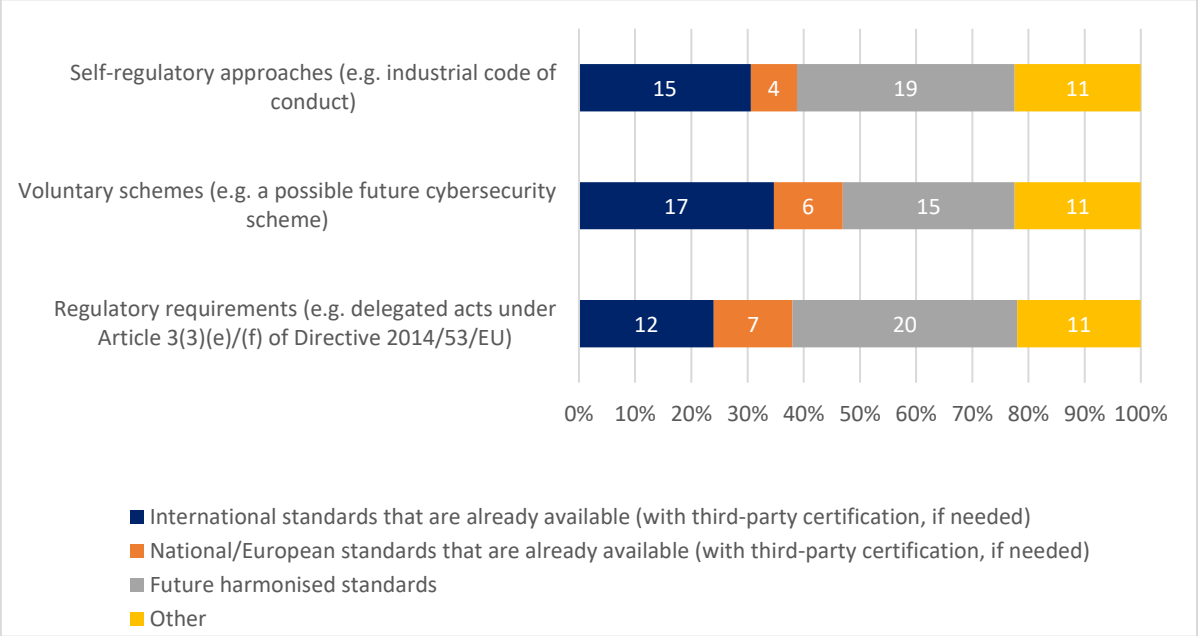


**Table 11: Preferred standards under delegated acts**

| Approaches: | International standards | National / EU standards | Future harmonised standards | Other |
|---|---|---|---|---|
| Self-regulatory approaches (e.g. industrial code of conduct) | 29% | 7% | 40% | 24% |
| Voluntary schemes (e.g. a possible future cybersecurity scheme) | 31% | 11% | 33% | 24% |
| Regulatory requirements (e.g. delegated acts under Article 3(3)(e)/(f) of Directive 2014/53/EU) | 20% | 13% | 42% | 24% |

## 4.5 Ease of implementation

As would be expected, the no-change option was reported to be the easiest to implement, with only 6% reporting that it would be difficult or somewhat difficult. The self-regulatory approach was considered relatively easy by two-thirds of respondents. Whilst the regulatory options (2, 3, 4) were considered to be more difficult to implement than the self-regulatory approach, fewer than half of respondents believed that they would be difficult or somewhat difficult.

Only a small proportion of respondents thought that new regulatory requirements on both data and privacy and on protection from fraud (Option 4) would be more difficult than introducing new requirements in only one area (Options 2 and 3).

**Figure 22: Ease of implementing each option**

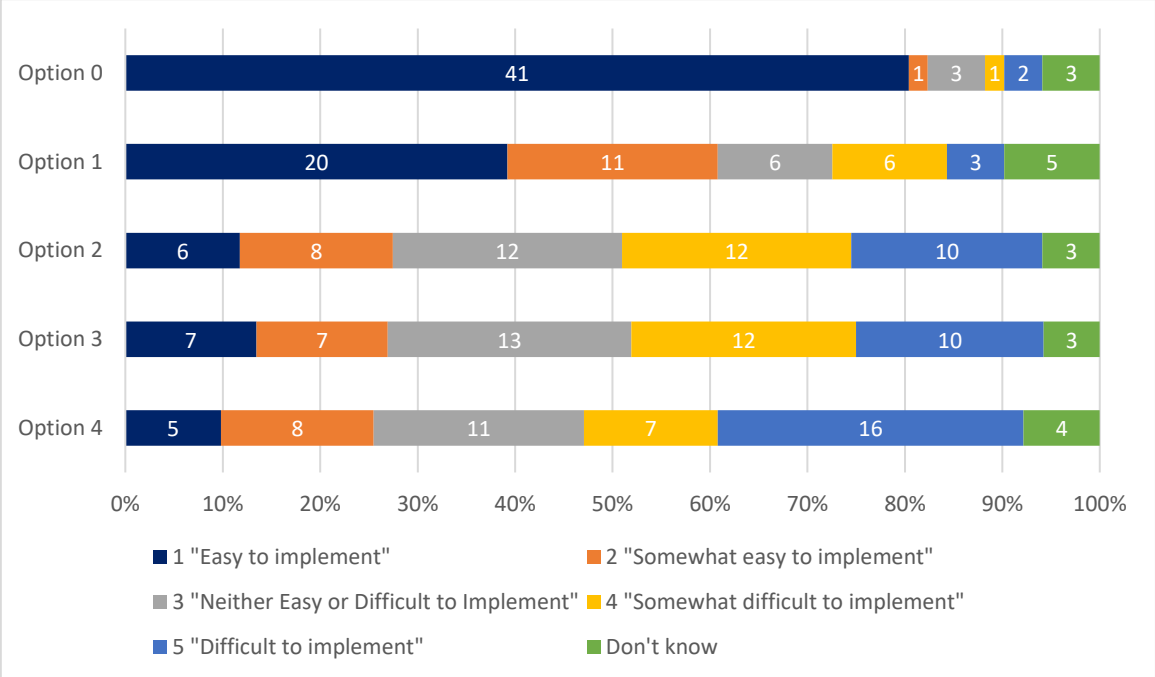


**Table 12: Ease of implementation**

| Regulatory options | 1 Easy | 2 Somewhat easy | 3 Neither easy nor difficult | 4 Somewhat difficult | 5 Difficult | Don't know |
|---|---|---|---|---|---|---|
| 1 No change | 80% | 2% | 6% | 2% | 4% | 6% |
| 2 Industry self-regulation | 39% | 22% | 12% | 12% | 6% | 10% |
| 3 Regulatory requirement on data and privacy | 12% | 16% | 24% | 24% | 20% | 6% |
| 4 Regulatory requirement on protection from fraud | 13% | 13% | 25% | 23% | 19% | 6% |
| 5 Regulatory requirement on data and privacy and protection from fraud | 10% | 16% | 22% | 14% | 31% | 8% |

When asked to comment on their response, several stakeholders restated the view that protection should be ensured by baseline requirements under horizonal EU legislation covering all products on the market, not just those covered by the RED. For example, the GDPR already requires manufacturers to implement safeguards to protect the privacy of users by requiring explicit consent before personal data can be collected and processed. However, two consumer organisations highlighted a potential difficulty in that the GDPR does not have the appropriate enforcement measures to enable market authorities to withdraw insecure products that could compromise data protection and / or privacy from the market.

One respondent suggested that a self-regulatory approach would be more difficult to implement than a regulatory approach because of the wide variety of products available on the market. In contrast, another respondent suggested that a voluntary or self-regulatory approach could respond more quickly to new threats and technological developments.

Two respondents suggested that a regulatory approach would be feasible provided that appropriate standards are developed. One of those recommended that consideration should be given as to whether existing international standards could be used to demonstrate conformity.

Several respondents stated that they could not comment on the ease of implementation and applicability without knowing the details of any requirements under delegated acts.

# 5. Impacts of the different options

In line with the Better Regulation Guidelines, the targeted consultation considered the impacts of the different policy options, including costs and benefits. Feedback on these questions was sought from the economic operators that responded to the targeted consultation. It should be noted that only economic operators provided were asked to provide feedback on costs. Stakeholder feedback on administrative costs and burdens for other stakeholders, notably market surveillance authorities, was solicited through the interview programme.

There were 28 respondents to these questions from the total sample of 56 to the targeted consultation overall. These responses were supplemented by undertaking detailed product case studies and by organising additional interviews with manufacturers linked to these cases.

## 5.1 Costs

### 5.1.1 Administrative costs

The economic operators 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. Only 1 out of 28 said that there would be no change.

**Figure 23: Administrative burden of new regulatory requirements (data protection & privacy)**

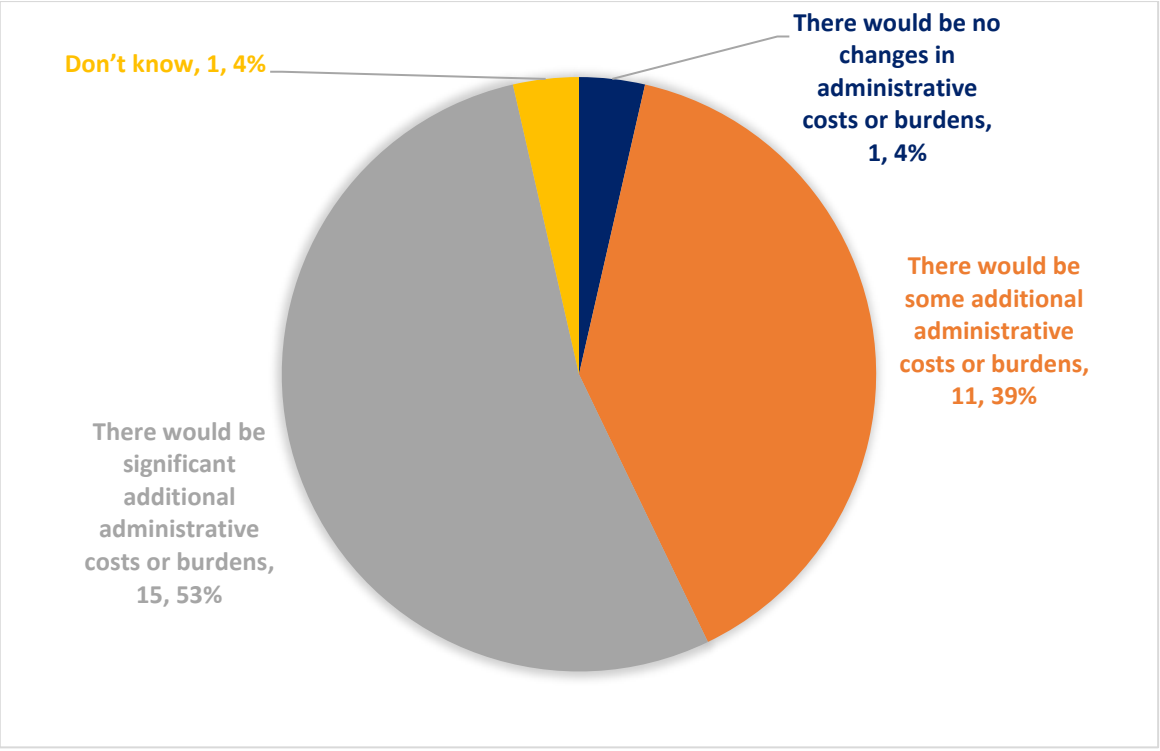
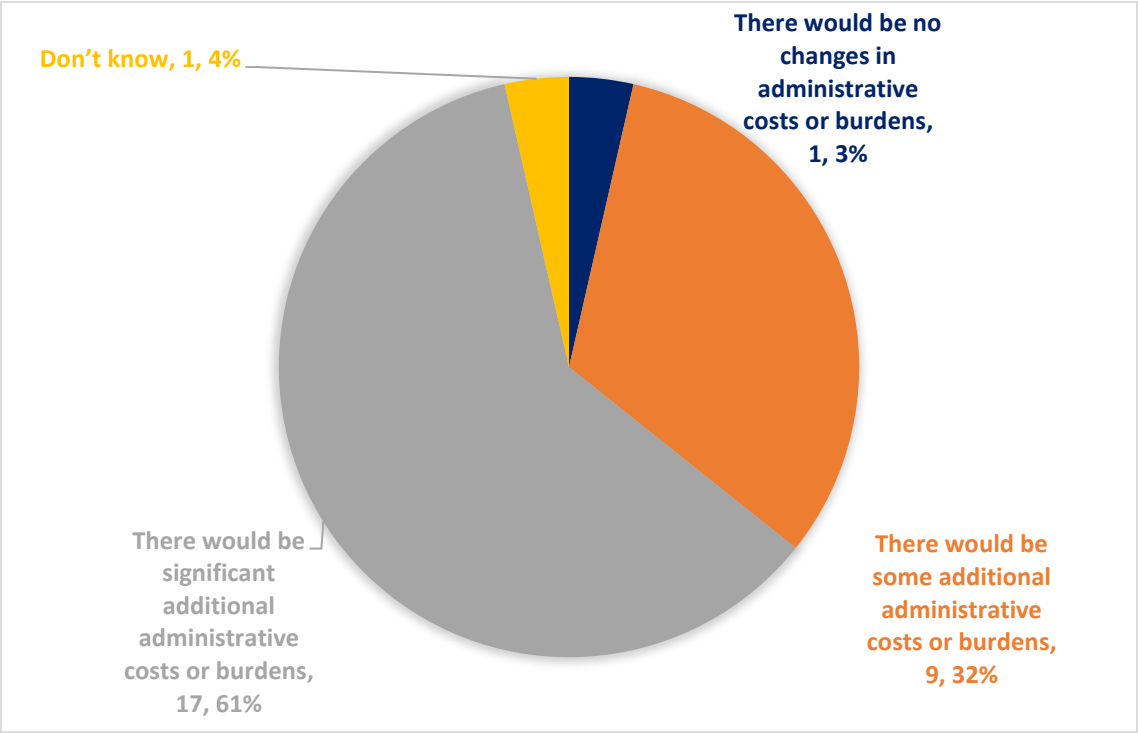


**Figure 24: Administrative burden of new regulatory requirements (fraud)**




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 Radio Equipment Directive 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 the following:

- costs of different applicable legal acts, standards applicable and conformity assessment procedures (3 respondents);
- third-party certification costs (2 respondents);
- lack of harmonised standards (1 respondent).

The firms that expected to incur each type of administrative cost were asked to comment on the degree of such costs, as show in the table below.

**Figure 25: Types of administrative burden incurred by firms**

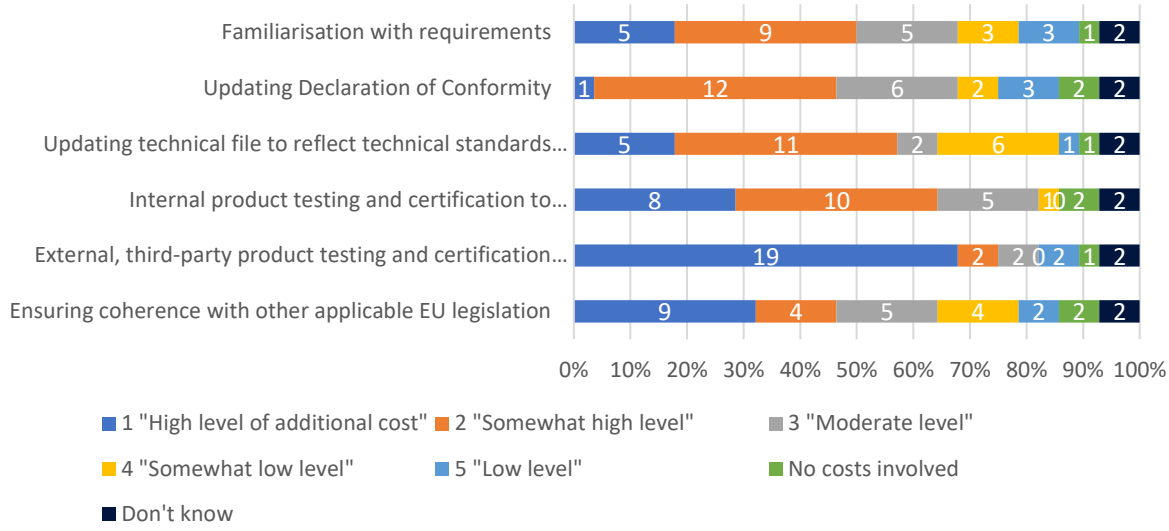



**Table 13: Level of administrative cost associated with different compliance processes**

| | 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% |

### 5.1.2 Compliance costs

The economic operators were asked whether the adoption of new regulatory requirements would lead to an increase in "substantive compliance costs". These were defined as "costs to embed requirements from the outset of the design process, such as research and development and innovation activities to ensure that 'security by design and default' principles are taken into account". Examples of substantive compliance costs would include redesigning a chip to ensure that data gathered can be anonymised or redesigning a product so that a unique password is generated rather than a generic password.

Of the 28 economic operators responding to this question, the majority (22 or 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 new compliant products.

In respect of research and development costs, two German manufacturers operating internationally believed that the extent of substantive compliance costs would depend on whether existing cybersecurity features already incorporated into products 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.

One 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 26: Incidence of substantive compliance costs**

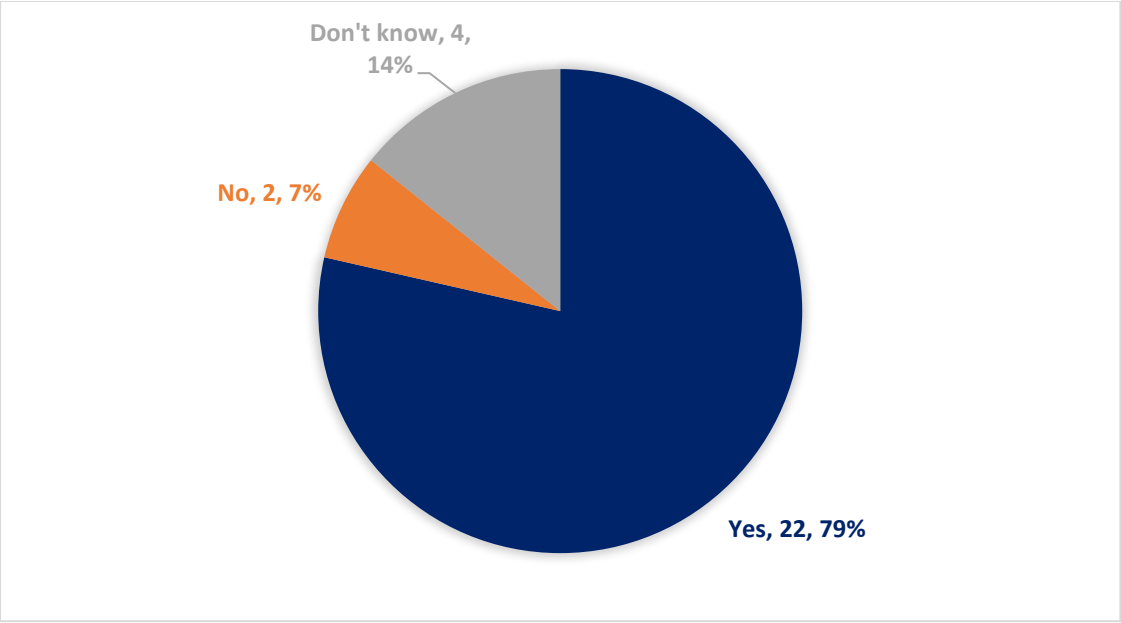


**Figure 27: Research and development costs to redesign chipsets or components**

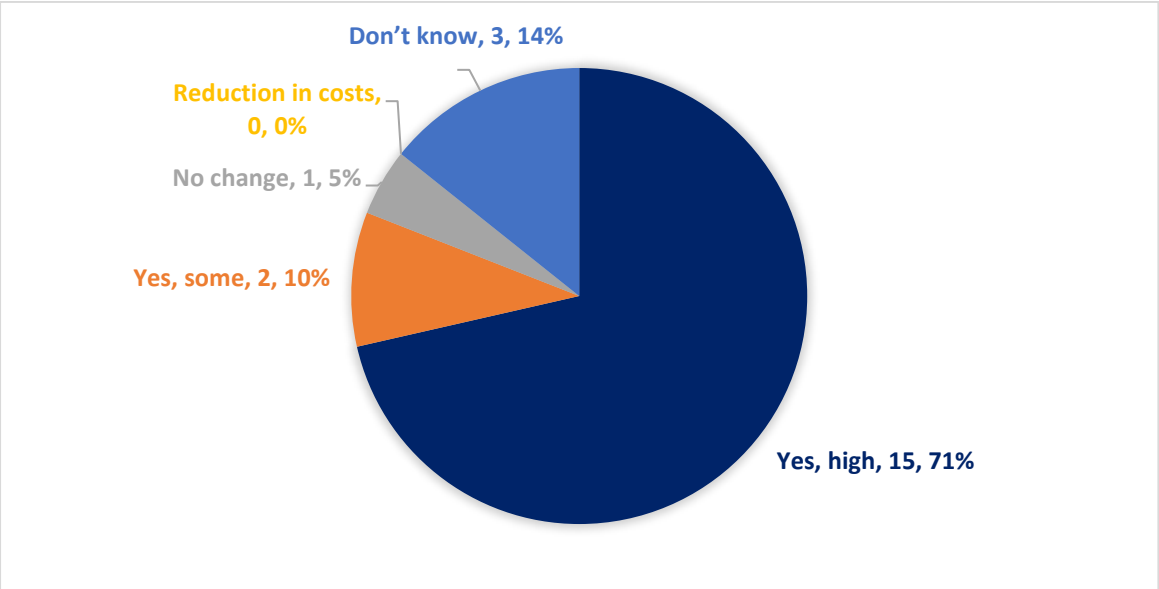
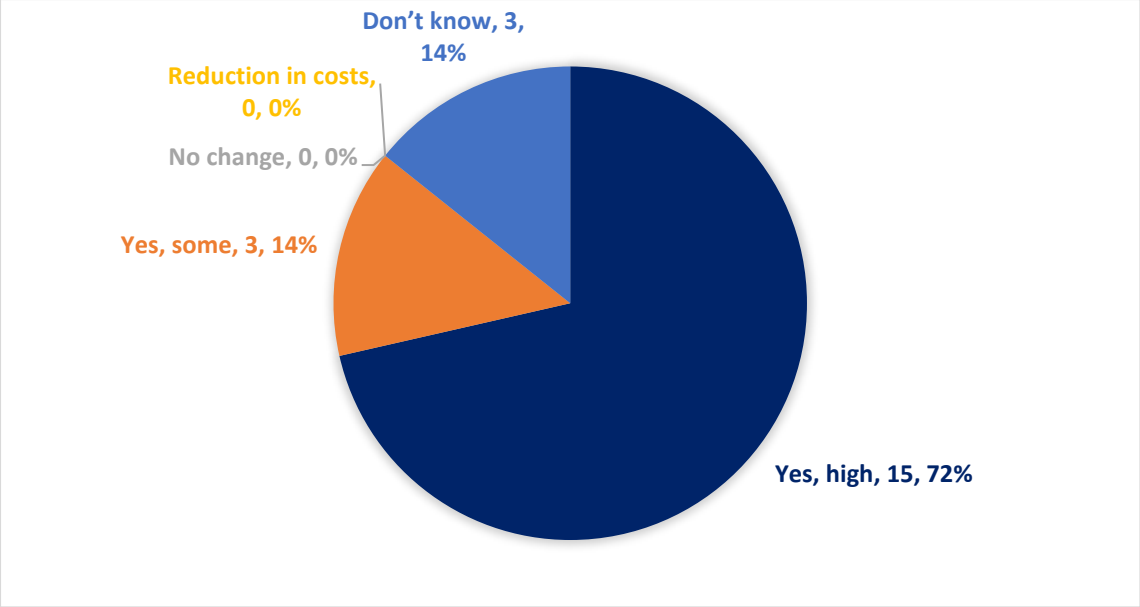



**Figure 28: Research and development costs to redesign products**




## 5.2 Effects of new regulatory requirements

### 5.2.1 Overall benefit for consumers

Stakeholders were asked to what extent consumers in general, and children and vulnerable consumers in particular, would benefit from the adoption of new regulatory requirements under the RED in respect of data protection and privacy, and protection from fraud. However, only four out of 56 stakeholders (7%) chose to respond to these questions.

Regarding the extent to which consumers in general and children and vulnerable consumers in particular would benefit, they reported as follows:

- Two consumer organisations: “to a great extent” (1/5);
- One research institute: “not at all” (5/5).
- One university: “to a very low extent” 4/5).

### 5.2.2 Benefits of a regulatory approach

The stakeholders were asked whether they believed there would be potential benefits as a result of the adoption of new regulatory requirements.

As shown in the figure below, **a majority of respondents anticipated a range of benefits**, including:

- increased legal certainty;
- increased protection for consumers;
- increased trust in digitisation;
- improved harmonisation of the internal market;
- level playing field for products (notwithstanding the concerns raised earlier about the risk of differentiating in regulatory terms between wireless and wired products); and
- a more coherent EU policy and legal framework.

There was, however, a divergence of views amongst the different stakeholders.

- **Economic operators tended not to anticipate such benefits**; no more than 25% anticipated each of the potential benefits to be significant (1/5), good (2/5) or some (3/5). No more than 6% anticipated any of the benefits to be significant (1/5).
- **All other types of stakeholder strongly anticipated such benefits** (i.e. compliance assessment bodies, national public administrations, consumer organisations, academia, law firms): at least 87% of such stakeholders (and in most cases 95%) expected anticipated each of the potential benefits to be significant (1/5), good (2/5) or some (3/5).

When asked to comment on benefits resulting from adoption of regulatory requirements (delegated acts) under the RED, all the stakeholders that responded merely restated general arguments for or (in more cases) against the adoption of such requirements.

**Figure 29: Potential benefits of regulatory requirements**

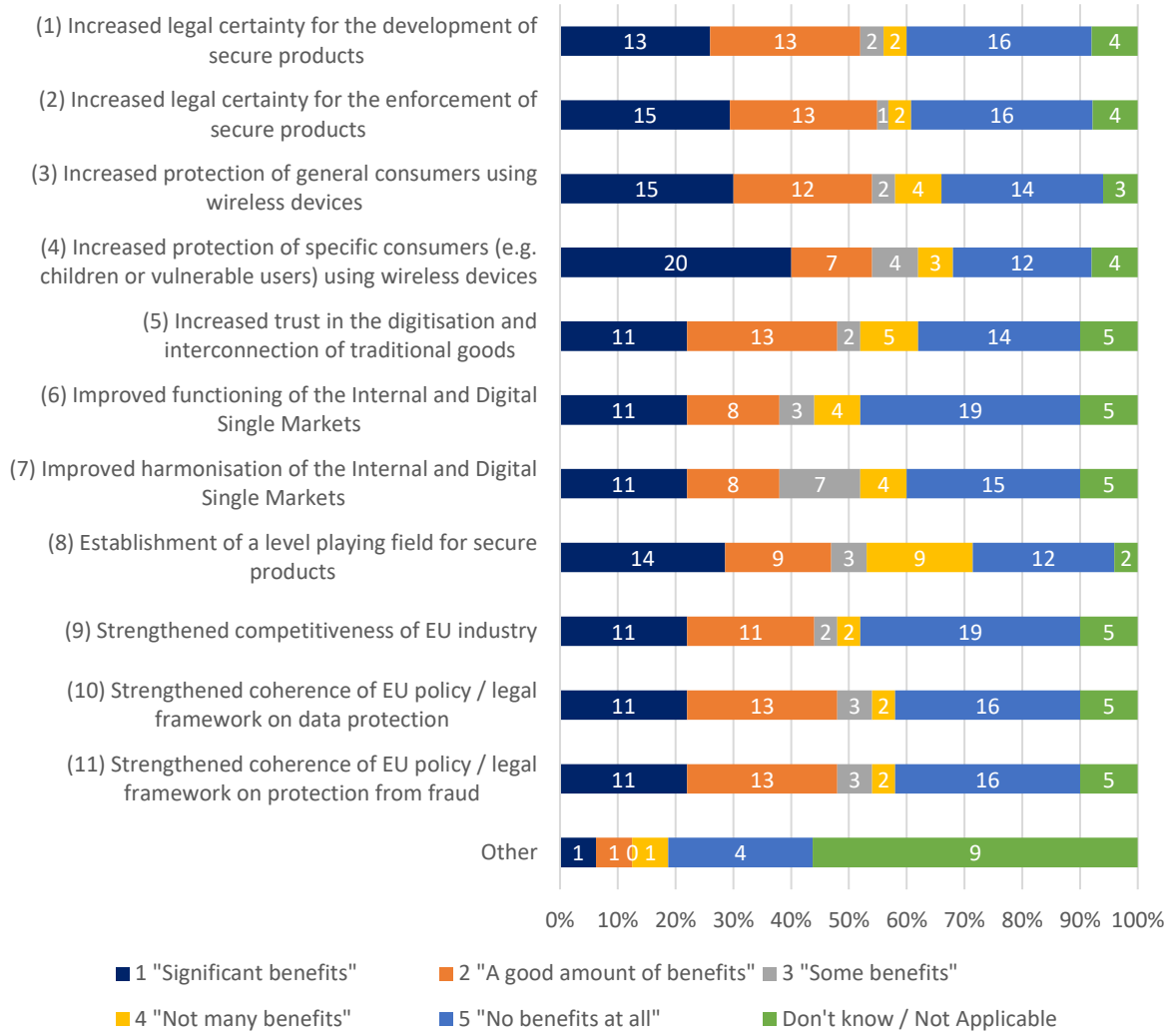


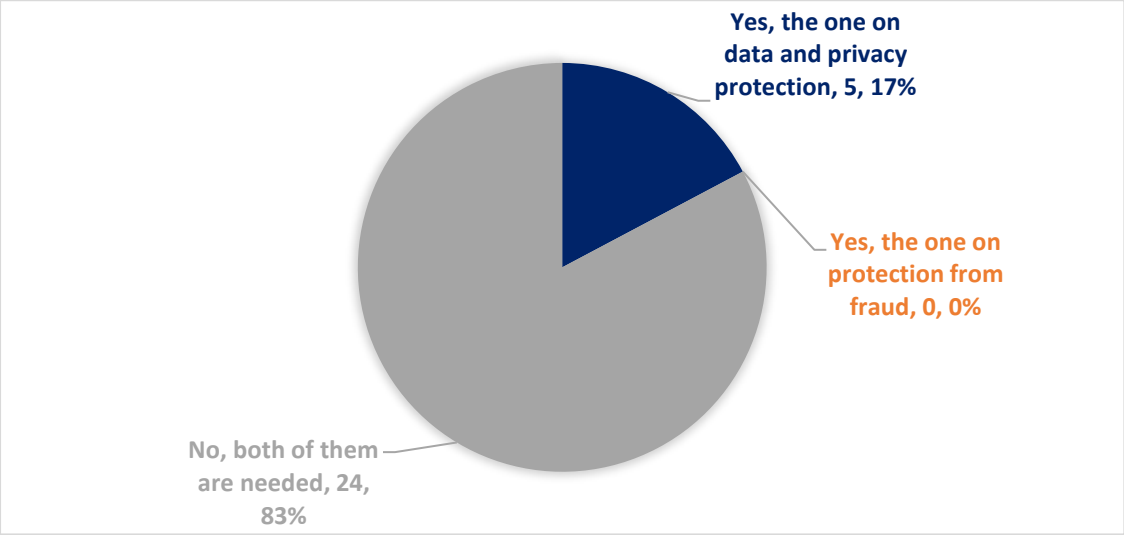

**Table 14: Potential benefits of regulatory requirements**

| Potential benefits | 1 "Significant benefits" (%) | 2 "A good amount of benefits" (%) | 3 "Some benefits" (%) | 4 "Not many benefits" (%) | 5 "No benefits at all" (%) | Don't know / Not Applicable (%) | Did not answer (number of respondents) |
|---|---|---|---|---|---|---|---|
| (1) | 23% | 23% | 4% | 4% | 29% | 7% | 6 |
| (2) | 29% | 25% | 2% | 4% | 31% | 8% | 5 |
| (3) | 30% | 24% | 4% | 8% | 28% | 6% | 6 |
| (4) | 40% | 14% | 8% | 6% | 24% | 8% | 6 |
| (5) | 22% | 26% | 4% | 10% | 28% | 10% | 6 |
| (6) | 22% | 16% | 6% | 8% | 38% | 10% | 6 |
| (7) | 22% | 16% | 14% | 8% | 30% | 10% | 6 |
| (8) | 29% | 18% | 6% | 18% | 24% | 4% | 7 |

| Potential benefits | 1 "Significant benefits" (%) | 2 "A good amount of benefits" (%) | 3 "Some benefits" (%) | 4 "Not many benefits" (%) | 5 "No benefits at all" (%) | Don't know / Not Applicable (%) | Did not answer (number of respondents) |
|---|---|---|---|---|---|---|---|
| (9) | 22% | 22% | 4% | 4% | 38% | 10% | 6 |
| (10) | 22% | 26% | 6% | 4% | 32% | 10% | 6 |
| (11) | 22% | 26% | 6% | 4% | 32% | 10% | 6 |
| Other | 6% | 6% | 0% | 6% | 25% | 56% | 40 |

Of those stakeholders that anticipated such benefits (of which only one quarter were economic operators), **the majority (83%) believed that both regulatory requirements were needed if the benefits were to be realised**.

**Figure 30: Extent to which benefits depend on regulatory requirements**




### 5.2.3 Harmonised standards

The overwhelming majority (88%) of **economic operators agreed that the availability of harmonised standards would reduce some of the costs or administrative burden** associated with new regulatory requirements. This was equally true of new requirement relating to data and privacy protection and to protection from fraud, with each operator offering an identical in respect of each requirement.

**Figure 31: Extent to which harmonised standards to demonstrate compliance for data and privacy protection would reduce some costs**

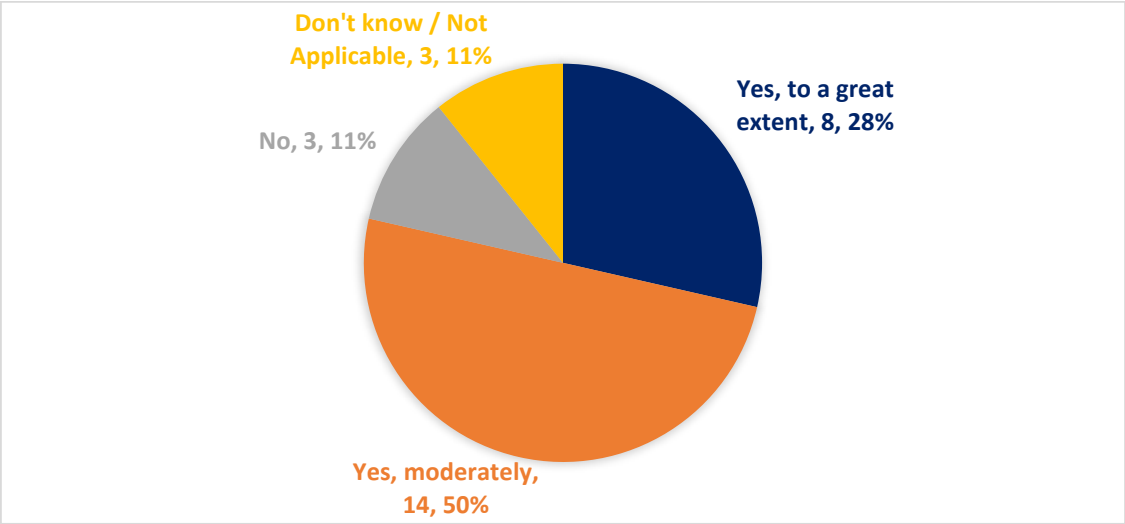
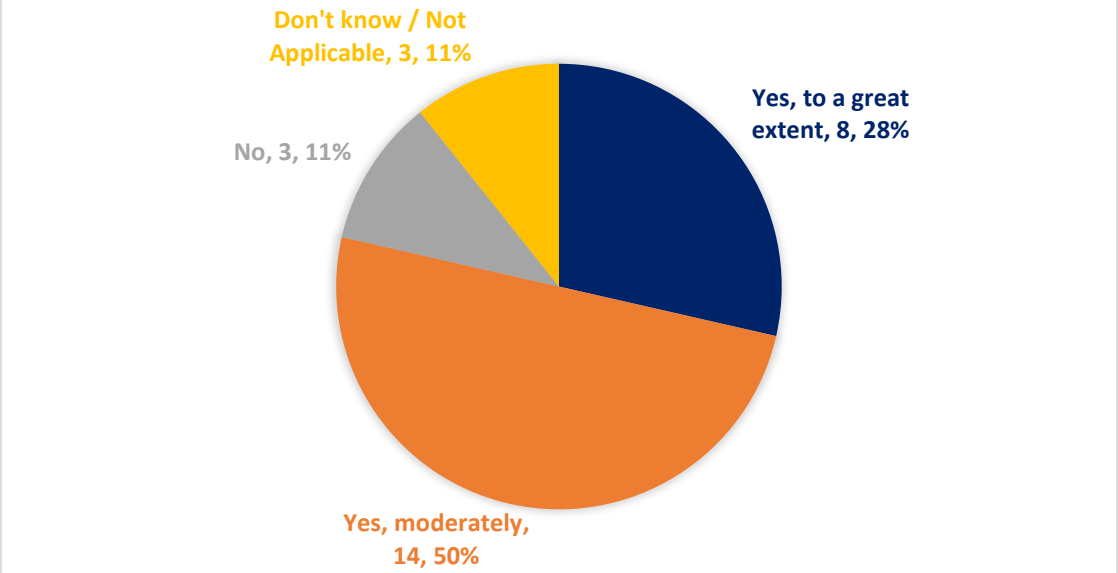



**Figure 32: Extent to which harmonised standards to demonstrate compliance for protection from fraud would reduce some costs**




### 5.2.4 Continued risks under a new regulatory approach

Stakeholders were asked how significant any continued risks would be under a new regulatory approach. Of those, providing a view:

- **Misuse of the network by means of radio equipment is considered a fairly significant risk**; 44% of respondents rated it as "significant" (1/5) or "fairly significant" (2/5); only 10% rated it as a very low risk(4/5) or not a risk at all (5/5);
- **Vulnerability to viruses, malware or other attacks** is considered a particularly significant risk; 60% of respondents rated it as "significant" (1/5) or "fairly significant" (2/5); only 8% rated it as a very low risk(4/5) or not a risk at all (5/5).

When asked to comment on their response, some respondents highlighted the inevitability of continued risks, given few pieces of technology are ever totally secure and that there is always the possibility of human error (e.g. users tricked into allowing an attacker to have access) or highly sophisticated attacks (e.g. by a nation state).

Two respondents also highlighted the continued risks of consumers having their products used in a botnet in the absence of any delegated act under Article 3 (3) d). Although out of formal scope, this is an issue which could be looked at in future studies in further detail.

**Figure 33: Continued risks under a new regulatory approach**

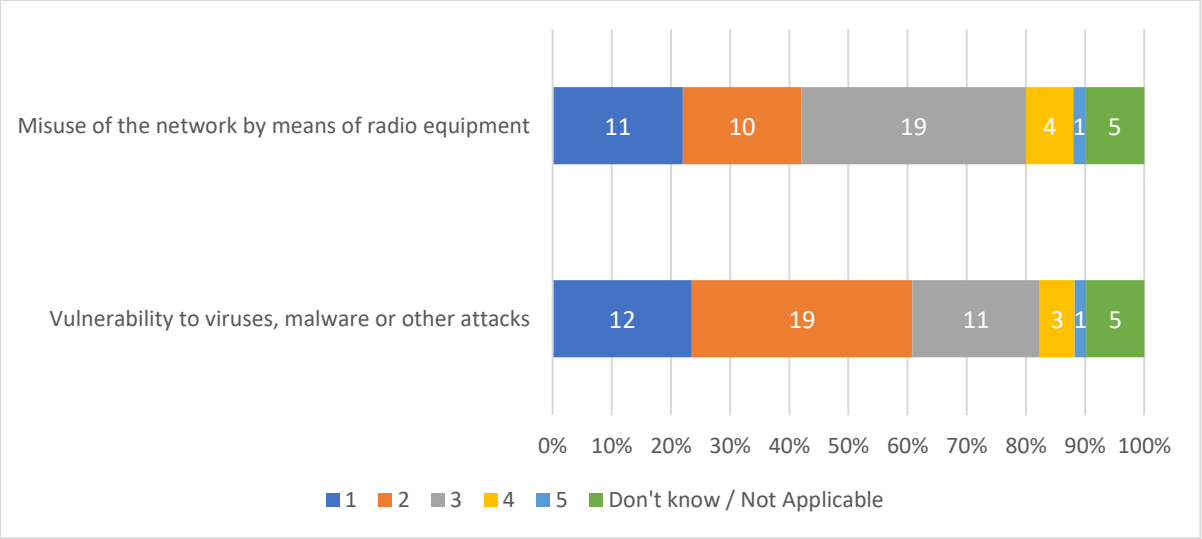



**Table 15: Number and percentage of respondents foreseeing continued risks**

| Possible risks | 1 | 2 | 3 | 4 | 5 | Don't know / Not Applicable |
|---|---|---|---|---|---|---|
| Misuse of the network by means of radio equipment | 11 (22%) | 10 (20%) | 19 (38%) | 4 (8%) | 1 (2%) | 5 (10%) |
| Vulnerability to viruses, malware or other attacks | 12 (24%) | 19 (37%) | 11 (22%) | 3 (6%) | 1 (2%) | 5 (10%) |

Respondents were asked how significant the exclusion of various products from new regulatory requirements would be from a risk perspective. As shown in the figure below, a **majority of respondents considered that the risks would be either significant or fairly significant for servers, desktops, printers, ethernet switches and other products**.

When asked to comment on the non-coverage of some non-radio products, most stakeholders offering a comment merely highlighted that such products are out of the RED's scope and, in any case, are subject to the requirements of other pieces of EU legislation.

One large non-EU manufacturer highlighted that wired devices can in effect operate as a wireless device, if they are plugged into a wireless device. In their opinion, this reinforces the principle that the method of connectivity (wired, wireless) should have little impact on the security and privacy requirements.

**Figure 34: Risks arising from exclusion of specific products**

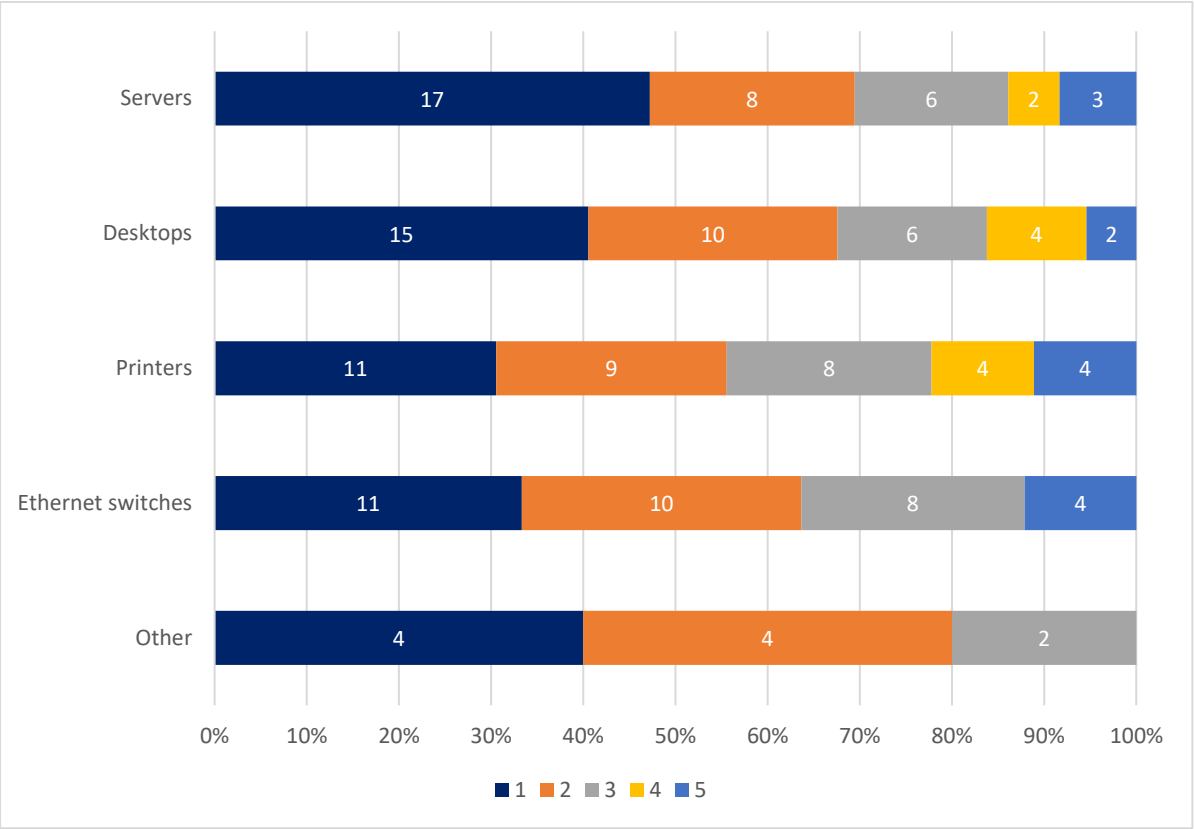



**Table 16: Risks arising from exclusion of specific products**

| Product type | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Servers | 47% | 22% | 17% | 6% | 8% |
| Desktops | 41% | 27% | 16% | 11% | 5% |
| Printers | 31% | 25% | 22% | 11% | 11% |
| Ethernet switches | 33% | 30% | 24% | 0% | 12% |
| Other | 40% | 40% | 20% | 0% | 0% |

### 5.2.5 Extent of different types of impacts

Respondents were asked their opinion on the extent to which different f impacts would arise as a result of the adoption of regulatory requirements under the RED. As shown in the figure below, a number of negative impacts are expected:

- **Increased administrative burden and costs in the value chain**: are expected to be "significant" or "a good amount" by more than 60% of respondents;
- Perhaps as a result, **consumers are expected to face increased costs**, expected to be "significant" or "a good amount" by more than 60% of respondents
- Manufacturers are expected to be less innovative and industry less competitive by more than 40% of respondents;

However, some potential negative impacts are expected to be modest:

- **National authorities expected only "some impact" on their administrative burden** (with the average score being 3/5 amongst the 10 authorities that responded).
- **EU legislation is expected to be only slightly more incoherent**; on average, respondents expected the impact to be less than "a good amount" (i.e. 2.5/5).

When asked to specify "other" potential impacts, one consumer organisation highlighted the increased security for consumers and the corresponding lower costs of consumer insecurity. For individuals, these include stolen data, financial loss, blackmail. For corporate consumers, such as hospitals, this includes less disruption to the provision of public services and less risks of outages and disruptions in service infrastructure.

**Figure 35: Potential impacts of regulatory requirements**

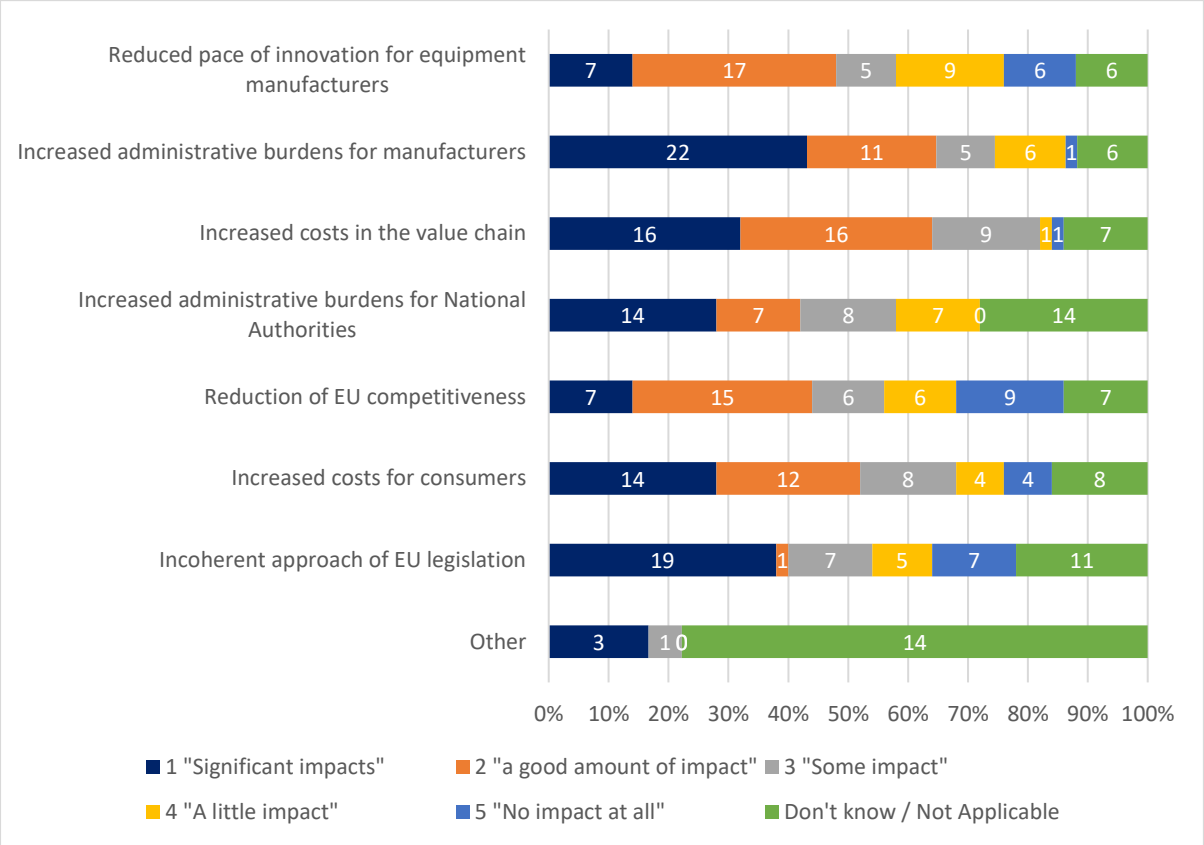
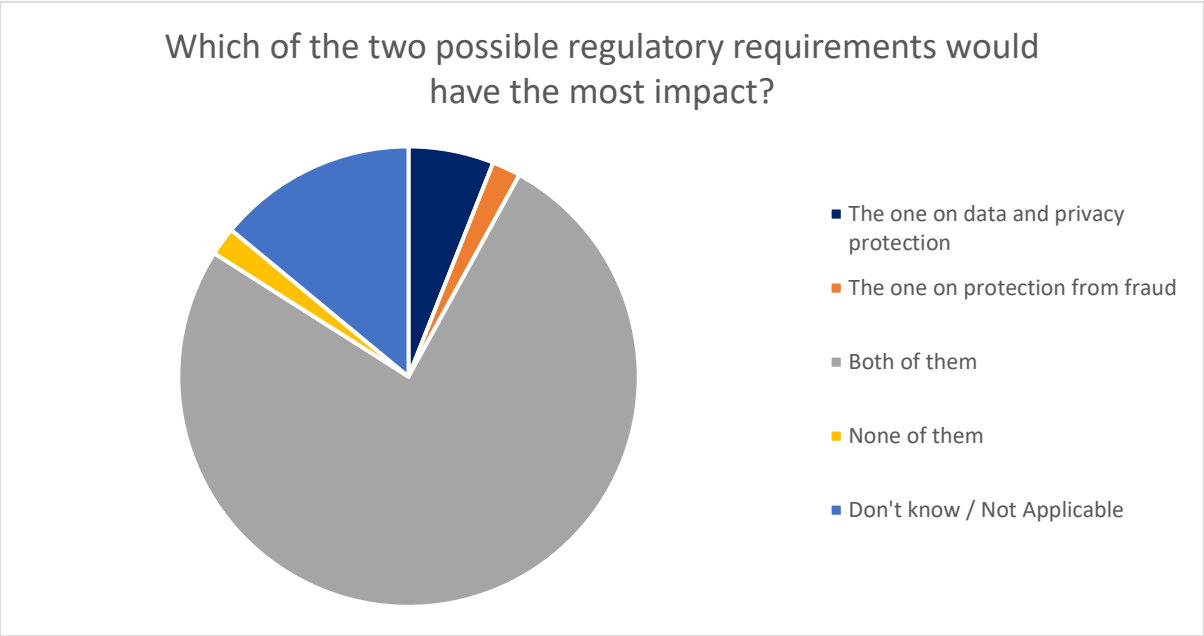


**Table 17: Potential impacts of regulatory requirements**

| Potential impacts | 1 "Significant impacts" | 2 "a good amount of impact" | 3 "Some impact" | 4 "A little impact" | 5 "No impact at all" | Don't know / Not Applicable | Did not answer (number of respondents) |
|---|---|---|---|---|---|---|---|
| Reduced pace of innovation for equipment manufacturers | 14% | 34% | 10% | 18% | 12% | 12% | 38 |
| Increased administrative burdens for manufacturers | 43% | 22% | 10% | 12% | 2% | 12% | 6 |
| Increased costs in the value chain | 32% | 32% | 18% | 2% | 2% | 14% | 6 |
| Increased administrative burdens for National Authorities | 28% | 14% | 16% | 14% | 0% | 28% | 6 |
| Reduction of EU competitiveness | 14% | 30% | 12% | 12% | 18% | 14% | 6 |
| Increased costs for consumers | 28% | 24% | 16% | 8% | 8% | 16% | 6 |
| Incoherent approach of EU legislation | 38% | 2% | 14% | 10% | 14% | 22% | 5 |
| Other | 17% | 0% | 6% | 0% | 0% | 78% | 6 |

**Figure 36: Type of regulatory requirement having the most impact**




As shown in the figure above, most stakeholders consider that the two possible regulatory requirements will have an equal impact. When asked to comment via an open question, all stakeholders that offered a response merely repeated general arguments in favour of, or against the adoption of such requirements.

## 5.3 Effects of a voluntary or self-regulatory approach

### 5.3.1 Benefits of a voluntary or self-regulatory approach

Stakeholders was asked about the extent to which various benefits would arise as a result of a voluntary or self-regulatory approach. Based on the number of respondents expecting benefits to be significant (1/5) or quite significant (2/5), **the most significant benefits are expected to be:**

- increased pace of innovation;
- absence of administrative burdens for manufacturers and national authorities;
- increased competitiveness of industry; and
- increased flexibility for the development of secure products.

When asked to list any other benefits, none of the respondents offered any suggestions.

**Figure 37: Expected benefits of a voluntary or self-regulatory approach**

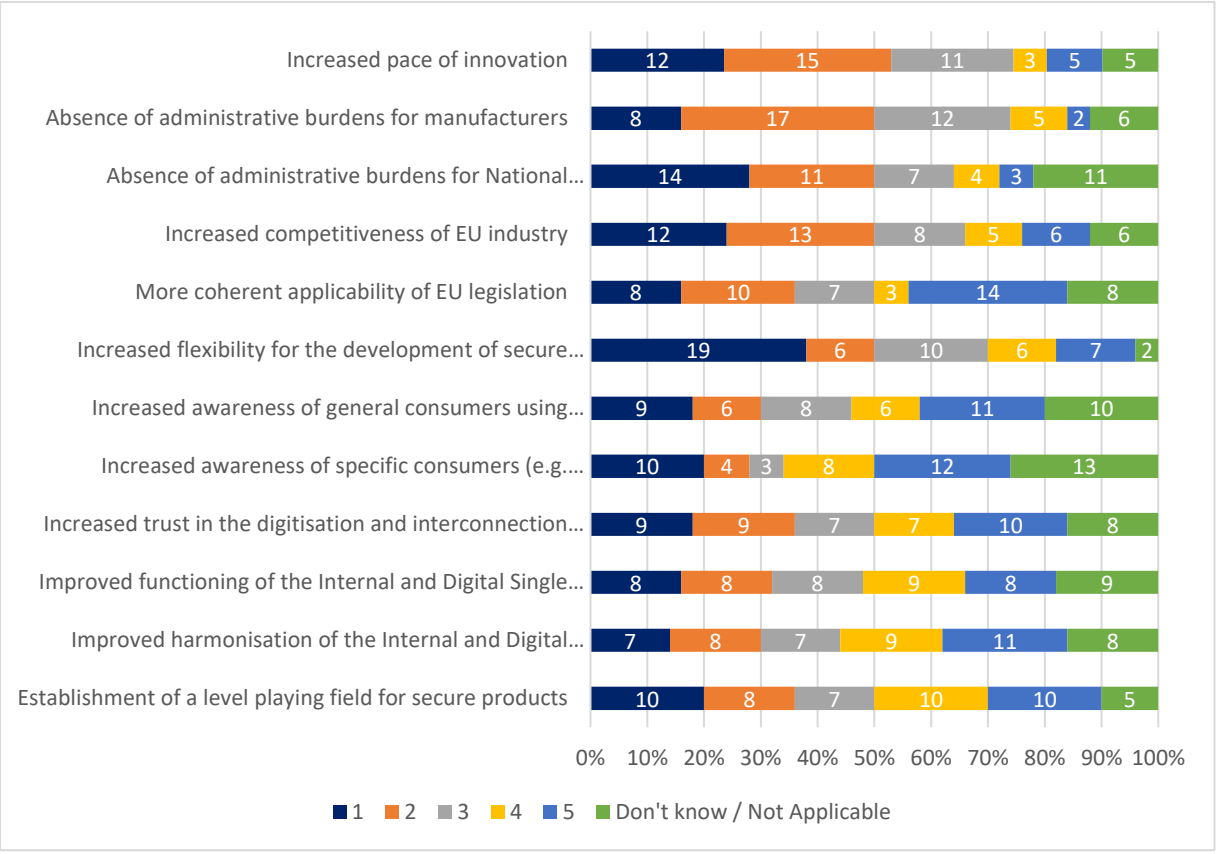


**Table 18: Percentage of respondents expecting benefits of a voluntary or self-regulatory approach**

| Possible benefits (1 = significant benefits; 5= no benefits at all) | 1 | 2 | 3 | 4 | 5 | Don't know / Not Applicable |
|---|---|---|---|---|---|---|
| Increased pace of innovation | 24% | 29% | 22% | 6% | 10% | 10% |
| Absence of administrative burdens for manufacturers | 16% | 34% | 24% | 10% | 4% | 12% |
| Absence of administrative burdens for National Authorities | 28% | 22% | 14% | 8% | 6% | 22% |
| Increased competitiveness of EU industry | 24% | 26% | 16% | 10% | 12% | 12% |
| More coherent applicability of EU legislation | 16% | 20% | 14% | 6% | 28% | 16% |
| Increased flexibility for the development of secure products | 38% | 12% | 20% | 12% | 14% | 4% |
| Increased awareness of general consumers using wireless devices | 18% | 12% | 16% | 12% | 22% | 20% |
| Increased awareness of children or vulnerable users using wireless devices | 20% | 8% | 6% | 16% | 24% | 26% |
| Increased trust in the digitisation and interconnection of traditional goods | 18% | 18% | 14% | 14% | 20% | 16% |
| Improved functioning of the Internal and Digital Single Markets | 16% | 16% | 16% | 18% | 16% | 18% |
| Improved harmonisation of the Internal and Digital Single Markets | 14% | 16% | 14% | 18% | 22% | 16% |
| Establishment of a level playing field for secure products | 20% | 16% | 14% | 20% | 20% | 10% |

### 5.3.2 Impacts of a voluntary or self-regulatory approach

Stakeholders was asked about the extent to which various negative impacts would arise as a result of a voluntary or self-regulatory approach.

The responses from stakeholders suggested that the negative impacts of a voluntary or self-regulatory approach will be modest. Indeed, one negative impact was expected to be significant (1/5) or quite significant (2/5) by more than 40% of respondents, namely weakened competitiveness of EU industry. The reason for this perception may be linked to the fact that some stakeholders perceive that a regulatory approach would allow European firms to gain a competitive advantage by being more cybersecure and paying greater attention to preventing data breaches which could lead to data protection and privacy being compromised and greater protection from fraud, which could be incorporated into product marketing and branding e.g. through the use of cybersecurity labelling.

When asked to specify “other” potential impacts of a voluntary or self-regulatory approach, one industry association suggested that this would lead to a less level playing field for European manufacturers. Another raised the risk that disreputable economic operators would not take part in voluntary measures or adhere to industry codes of conduct. Therefore, the level of voluntary compliance would be low and never apply and there would be no mechanism for ensuring enforcement.

One stakeholder suggested that an effective voluntary or self-regulatory approach could allow Europe to become a world-leader in this field, which would increase stakeholder involvement in developing, maintaining and verifying requirements, supporting the building of European expertise in the field of cybersecurity.

**Figure 38: Expected impacts of a voluntary or self-regulatory approach**

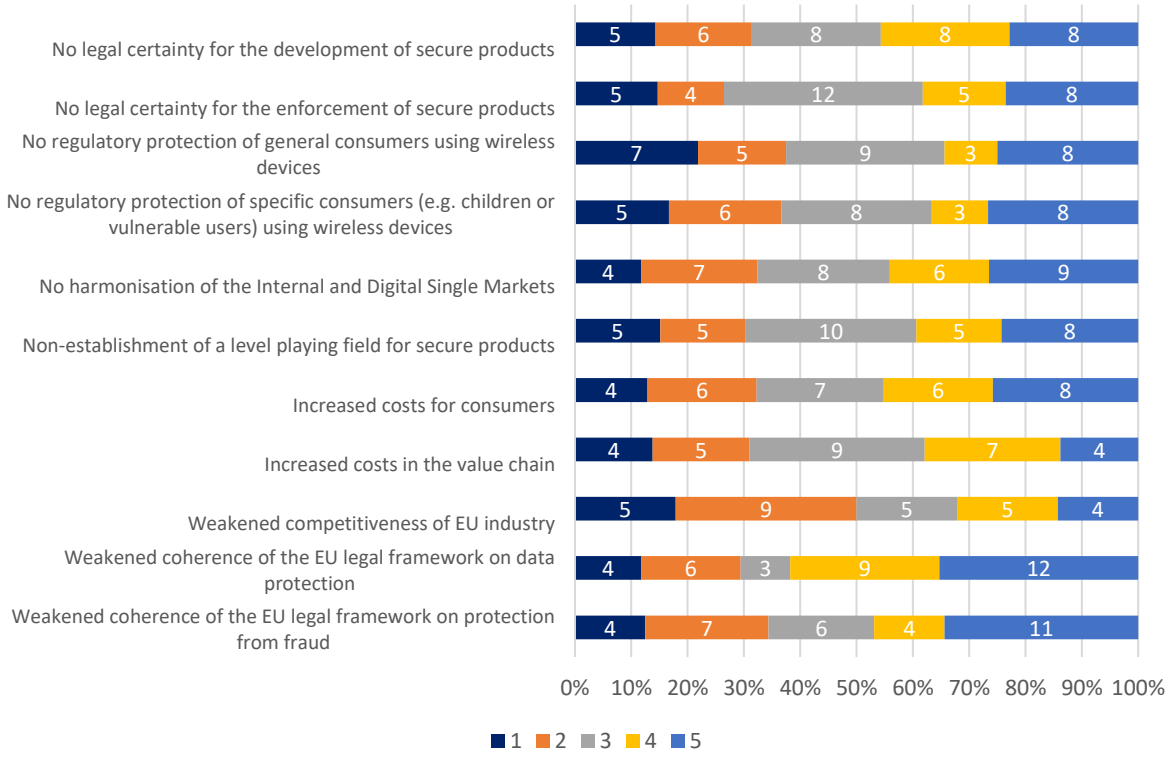



**Table 19: Percentage of respondents expecting benefits of a voluntary/self-regulatory approach**

| Possible impacts | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| No legal certainty for the development of secure products | 14% | 17% | 23% | 23% | 23% |
| No legal certainty for the enforcement of secure products | 15% | 12% | 35% | 15% | 24% |
| No regulatory protection of general consumers using wireless devices | 22% | 16% | 28% | 9% | 25% |
| No regulatory protection of specific consumers (e.g. children or vulnerable users) using wireless devices | 17% | 20% | 27% | 10% | 27% |
| No harmonisation of the Internal and Digital Single Markets | 12% | 21% | 24% | 18% | 26% |
| Non-establishment of a level playing field for secure products | 15% | 15% | 30% | 15% | 24% |
| Increased costs for consumers | 13% | 19% | 23% | 19% | 26% |
| Increased costs in the value chain | 14% | 17% | 31% | 24% | 14% |
| Weakened competitiveness of EU industry | 18% | 32% | 18% | 18% | 14% |
| Weakened coherence of the EU legal framework on data protection | 12% | 18% | 9% | 26% | 35% |

| Possible impacts | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Weakened coherence of the EU legal framework on protection from fraud | 13% | 22% | 19% | 13% | 34% |
| Other | 57% | 0% | 14% | 29% | 0% |

More than two-third of stakeholders expected economic, social or environmental benefits or impacts to result from the adoption of voluntary/self-regulatory requirements. However, when asked to describe the type and magnitude of any benefits or impacts, the stakeholders that responded all repeated general arguments in favour or against such an approach, rather than highlighting impacts not already mentioned.

**Figure 39**: **Respondents expecting economic, social or environmental benefits or impacts**