Centre for
Strategy & Evaluation
Services

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

Analysis of responses to the Open Public Consultation (OPC)

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 an open public consultation (OPC) regarding the likely costs and benefits of possible 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), for example, fall under this Directive. However, with the increasing number of radio equipment placed on the market and with the incoming advent of the "internet of things" (IoT), the European Commission considers it a priority to increase legal certainty for consumers, manufacturers and other stakeholders.

The OPC 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 invited any interested individual organisation to give an opinion on the questions at hand, regardless of their knowledge or experience in this field. The consultation was published online on 9th August 2019 and was open until 15th November 2019 on the Commission's "EUSurvey" tool.

In parallel to the OPC, a targeted consultation of stakeholders was also operated, which was open to industry associations, companies (including SMEs), consumers, enforcement authorities, etc. The results of the targeted consultation are the subject of a separate report (Annex 6).

1.2 Implementation of the consultation

A total of 42 respondents completed the on-line questionnaire. It should be noted that, given the open nature of the consultation, the sample is entirely self-selected and is not necessarily representative of the wider population of interested parties (e.g. citizens, businesses, public authorities). The results presented here cannot be interpreted as those of a survey but rather as the expression of the opinion of a number of citizens, businesses and other stakeholders with an interest in the potential risks related to wireless devices and the legal framework for mitigating such risks.

The online questionnaire consisted of 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. Some quoted comments have been translated from the source language or edited for reasons of grammar or spelling. Some responses to open questions were not relevant to the questions covered by the consultation and were therefore discarded.

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 represented 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.

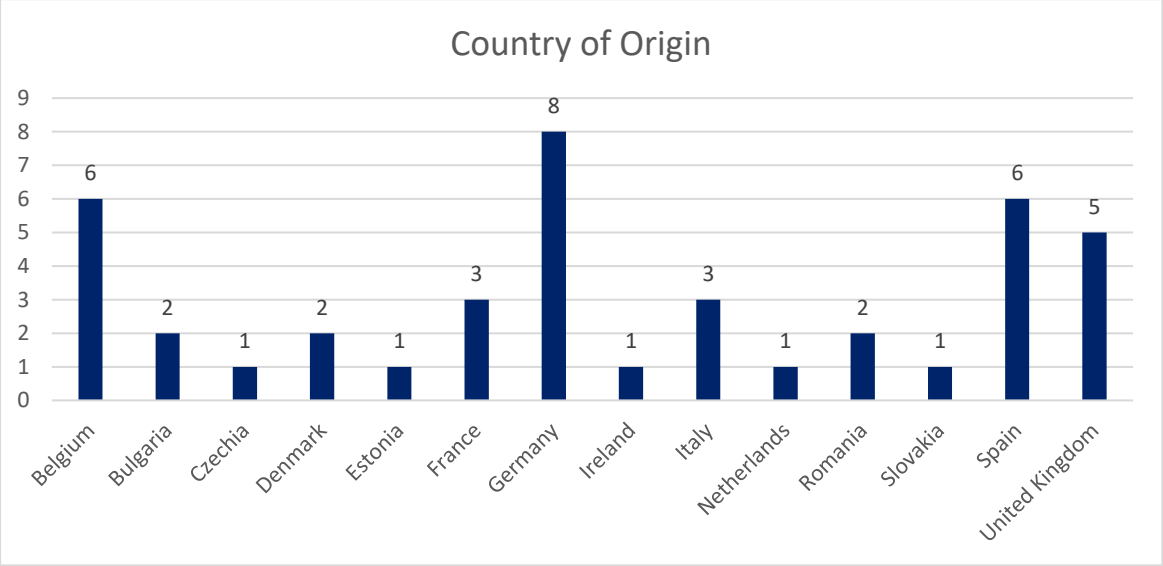
2. Profile of respondents

2.1 Country

The profile of respondents' country was as follows:

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

Figure 1 Respondents' country of origin



2.2 Type of respondent

The profile of the types of respondent was as follows:

- Of the 42 respondents, slightly more than half (22) were **citizens**.
- Citizens came from 10 of the 14 EU Member States represented amongst all respondents.
- Of the six **public authorities**, four were from Spain and one each from Estonia and Ireland.
- Of the seven **business associations**, five were EU-level bodies based in Belgium.
- The six **businesses** came from five different countries. Three were micro, two small and one large.
- The one **consumer** organisation was an EU-level body based in Belgium.

Figure 2 Type of respondent to the survey (numbers)

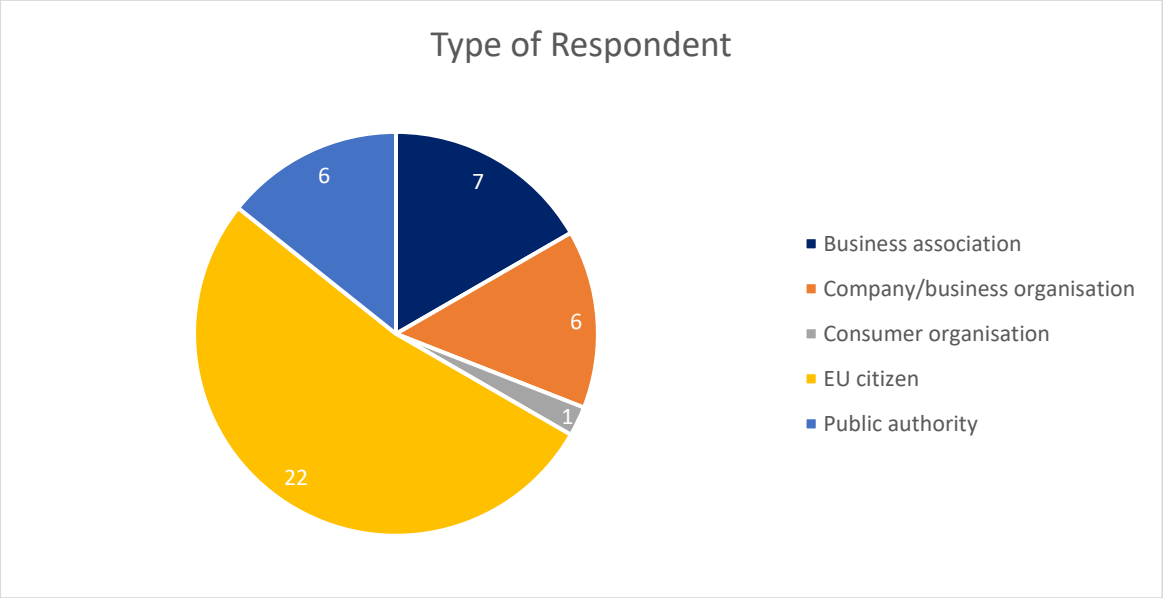
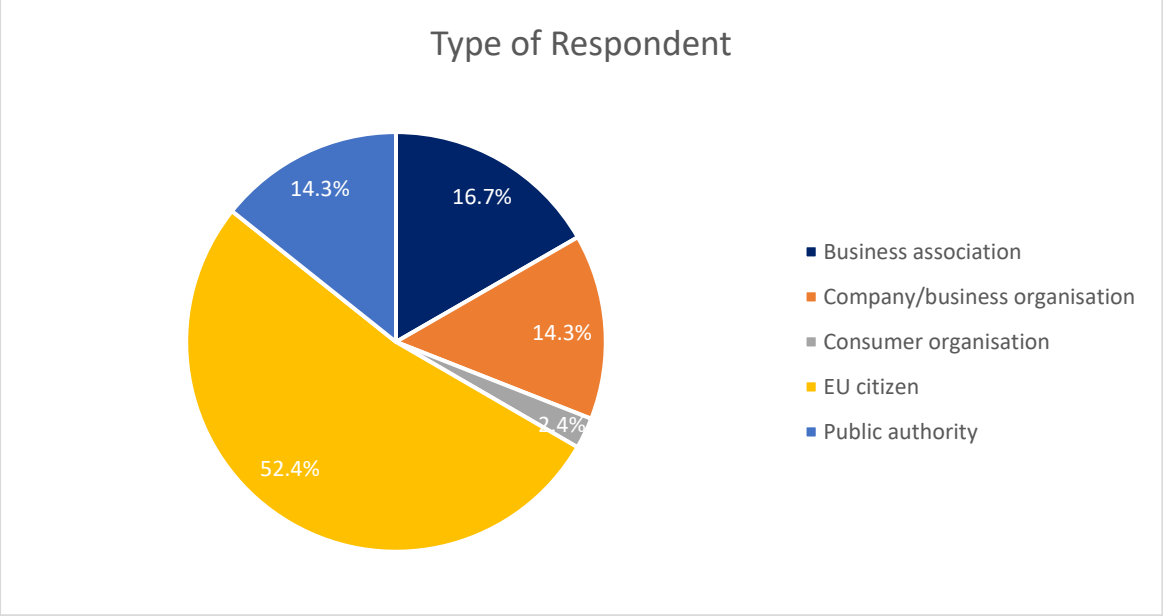


Figure 3 Type of respondent to the survey (percentages)



2.3 Size of organisation

The profile of the size of organisations (i.e. excluding citizens) was as follows:

- **Large** organisations (+250 people) were public authorities or businesses;
- **Medium** organisations (50-249 people) were national public authorities (Estonia, Ireland, Spain);
- **Small** organisations (10-49 people) were all business associations, except for one business;
- **Micro**-organisations (<10 people) included all types of organisation.

Figure 4 Size of organisations responding to the survey (number)

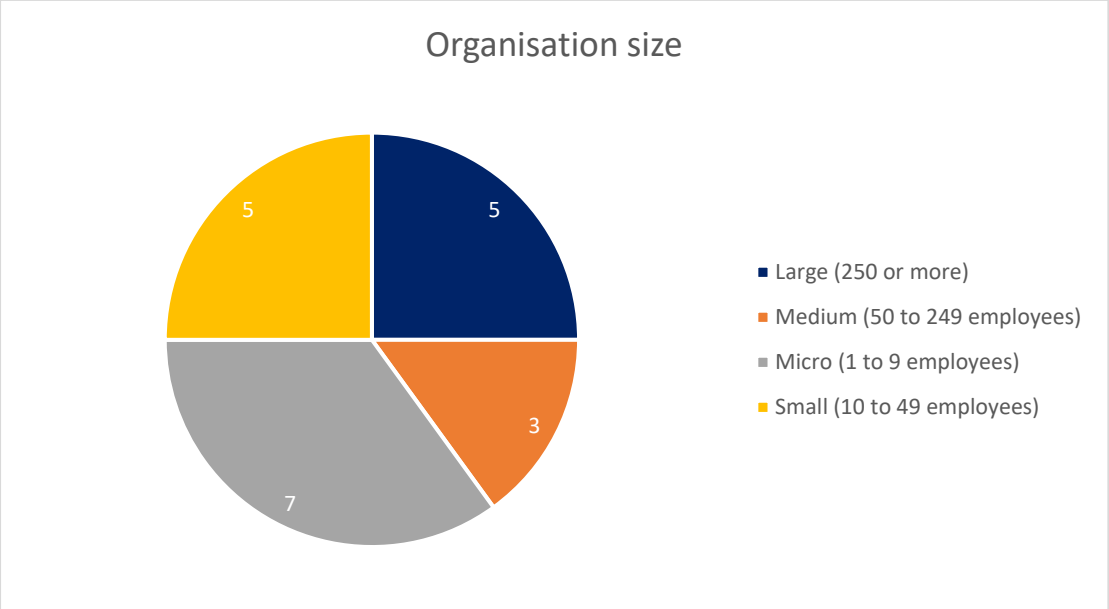
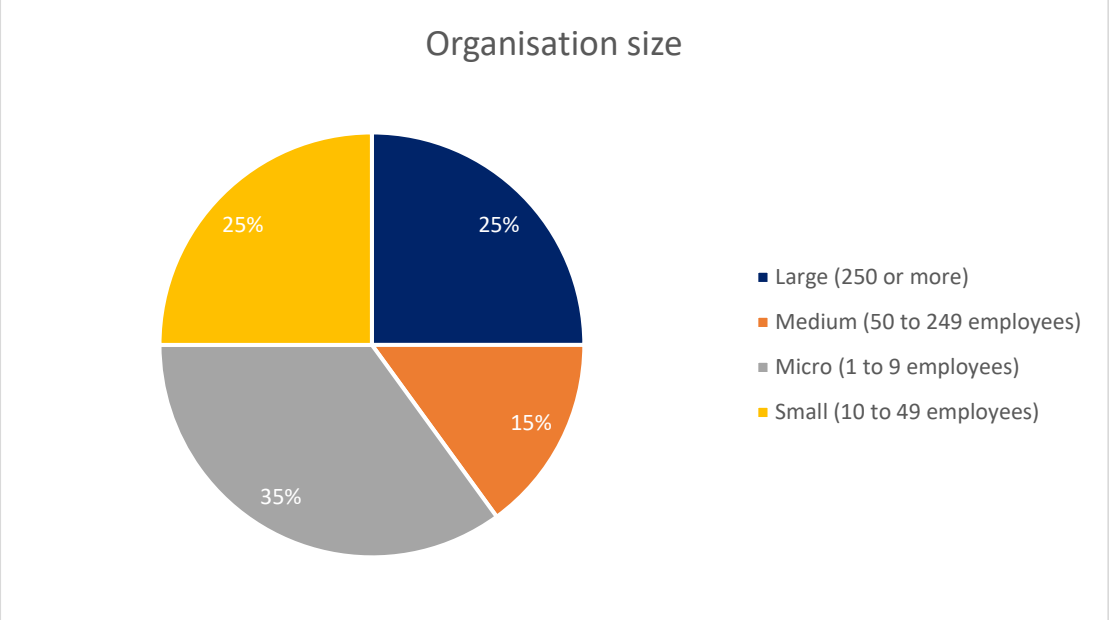


Figure 5 Size of organisations responding to the survey (percentages)

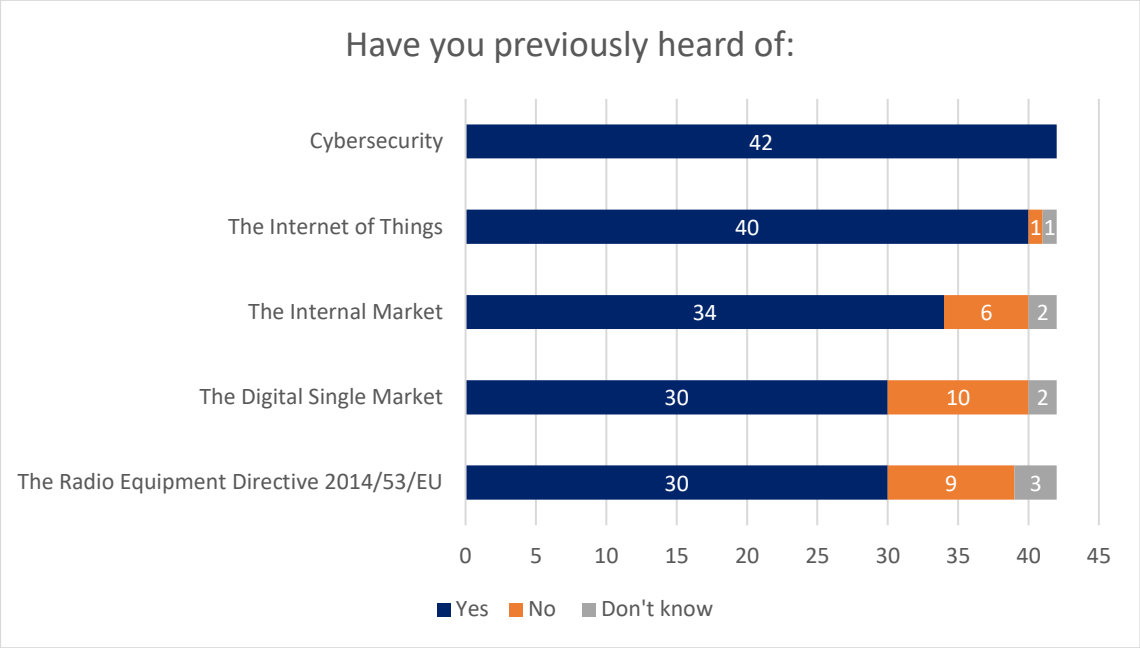


2.4 Respondents' prior knowledge of key issues

Respondents were asked to state whether they had previously heard of key issues related to the consultation. The chart below shows that:

- There was very high awareness of cybersecurity and the internet of things;
- A mix of citizens (4/8), businesses and one business association had not heard of the Internal Market (or did not know);
- A mix of citizens (6/12) and other types of respondent had not heard of the Digital Single Market (or did not know);
- Only citizens had not heard of the RED (or did not know), except for one business.

Figure 6 Respondents prior knowledge of key issues



3. Baseline position

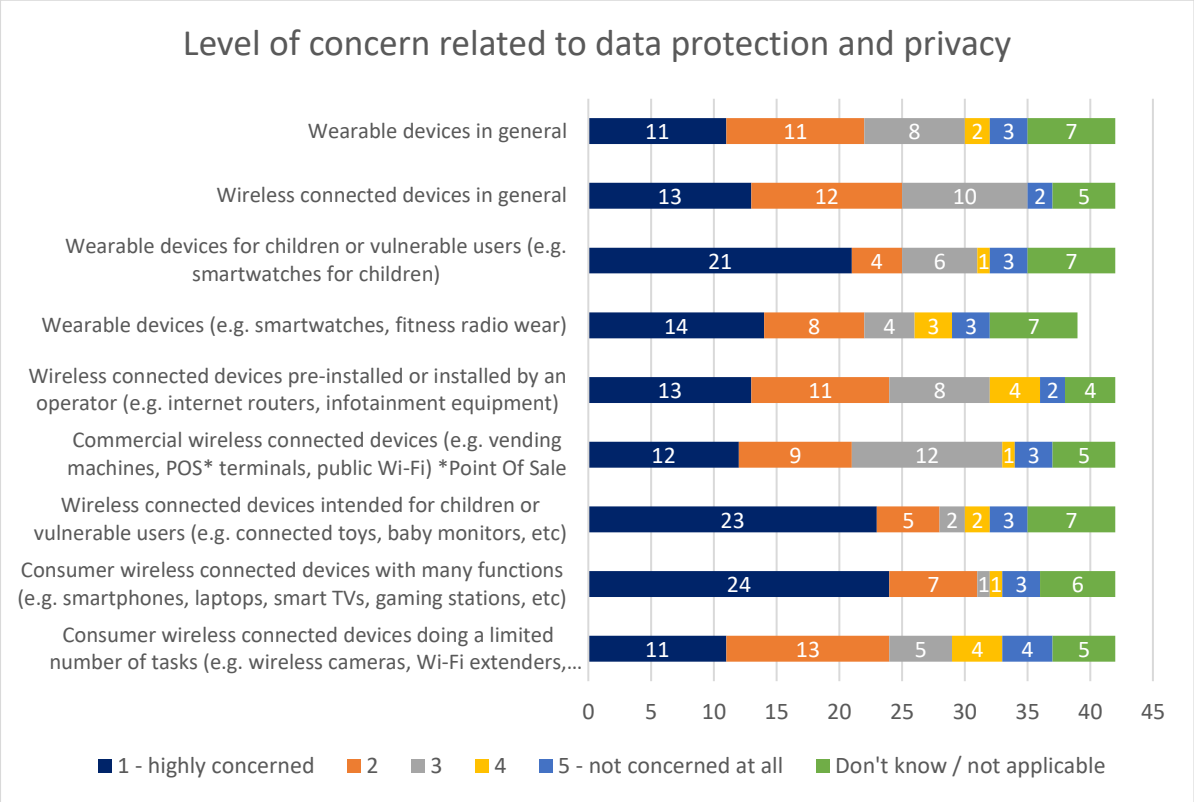
3.1 Level of concern regarding wireless internet-connected devices

Respondents were asked to state their level of concern regarding various types of connected wireless devices.

In respect of data protection and privacy, Figure 7 shows that:

- At least half of respondents were highly concerned (1/5) or fairly highly concerned (2/5) about all types of devices. Only 3 (7%) were not concerned at all.
- Wireless devices in general gave slightly more concern than wearable devices in general.
- Devices raising most concerns were consumer devices with many functions, e.g. smartphones, laptops, smart TVs, gaming stations.
- Next most concerning devices were wireless devices intended for children or vulnerable adults and wearable devices for children or vulnerable adults.
- Devices giving least concern were commercial devices (i.e. lowest number of 1 and 2 responses).

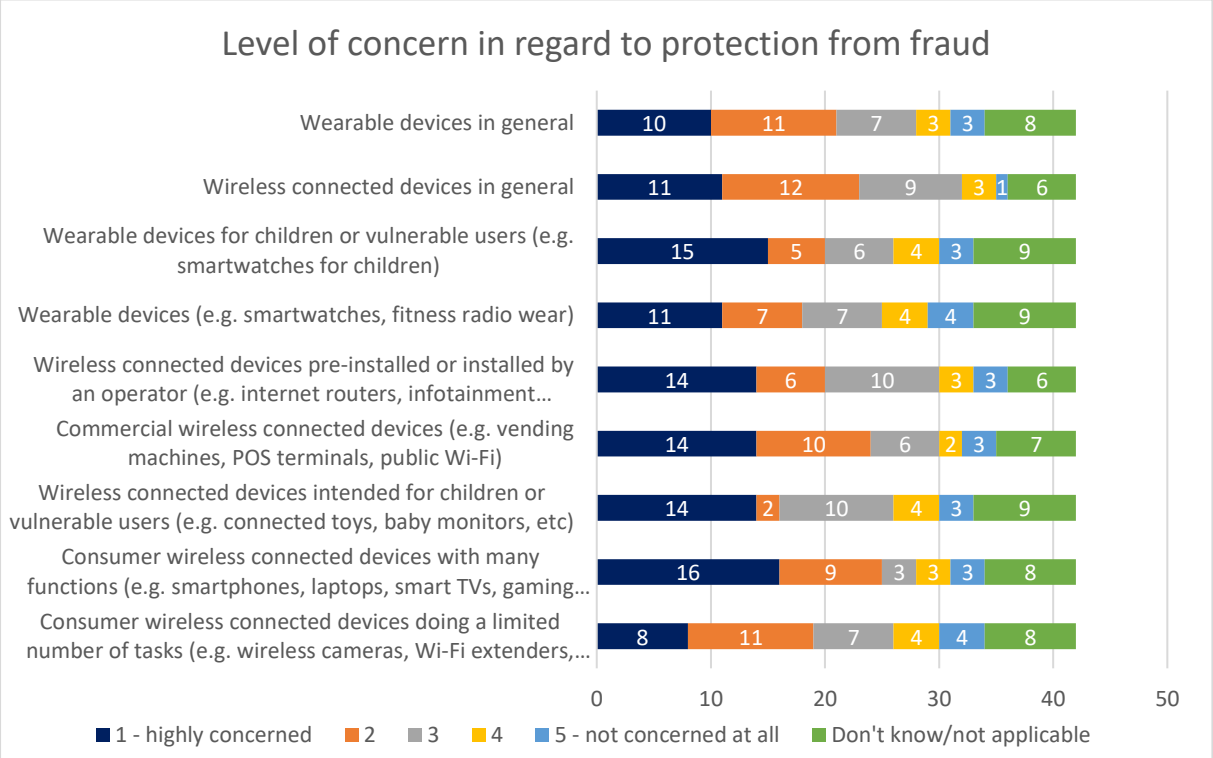
Figure 7 Level of concern regarding different types of devices (data protection and privacy)



In respect of data protection and privacy and protection from fraud, Figure 8 shows that:

- Respondents were less concerned about protection from fraud than about data protection and privacy, across all types of device;
- Wireless devices in general gave slightly more concern than wearable devices in general.
- Most concern was raised by consumer devices with many functions, e.g. smartphones, laptops, smart TVs, gaming stations.
- Next most concern was raised by commercial devices (e.g. vending machines, POS terminals, public Wi-Fi)
- Least concern was raised by wireless devices for children and vulnerable adults (i.e. lowest number of 1 and 2 responses).

Figure 8 Level of concern regarding different types of devices (protection from fraud)



The respondents were invited to identify other products or to elaborate on their replies. Four respondents highlighted specific products that gave them cause for concern:

- novel payment services;
- medical devices;
- intelligent virtual assistants (IVA);
- government-installed connected surveillance equipment;
- devices to capture operating data from construction machinery, e.g. operating times, fuel consumption, which can be at risk of being tampered with thus creating the risk of fraud.

Issues that raised particular concern included:

- Lack of requirements to force users to change ID and passwords from default settings.
- Importance of the GDPR in regulating collection and use of personal data.
- New security vulnerabilities are identified on a regular basis and regular updates may not be available or outdated hardware may be unable to be sufficiently protected and users may be left unaware.
- Need for improvement of connected devices (data protection and privacy and protection against fraud), particularly by preventing non-compliant products from entering the market.
- Importance of state-of-the art technical solutions to mitigate risks.
- Location of manufacturers or operators outside the EEA makes it difficult for regulators to enforce compliance.
- Volume of personal or sensitive data collected by devices used by children or vulnerable adults and potentially accessible to operators or third parties.
- Lack of firmware updates making devices increasingly vulnerable over time.[2]

3.2 Specific risks to users

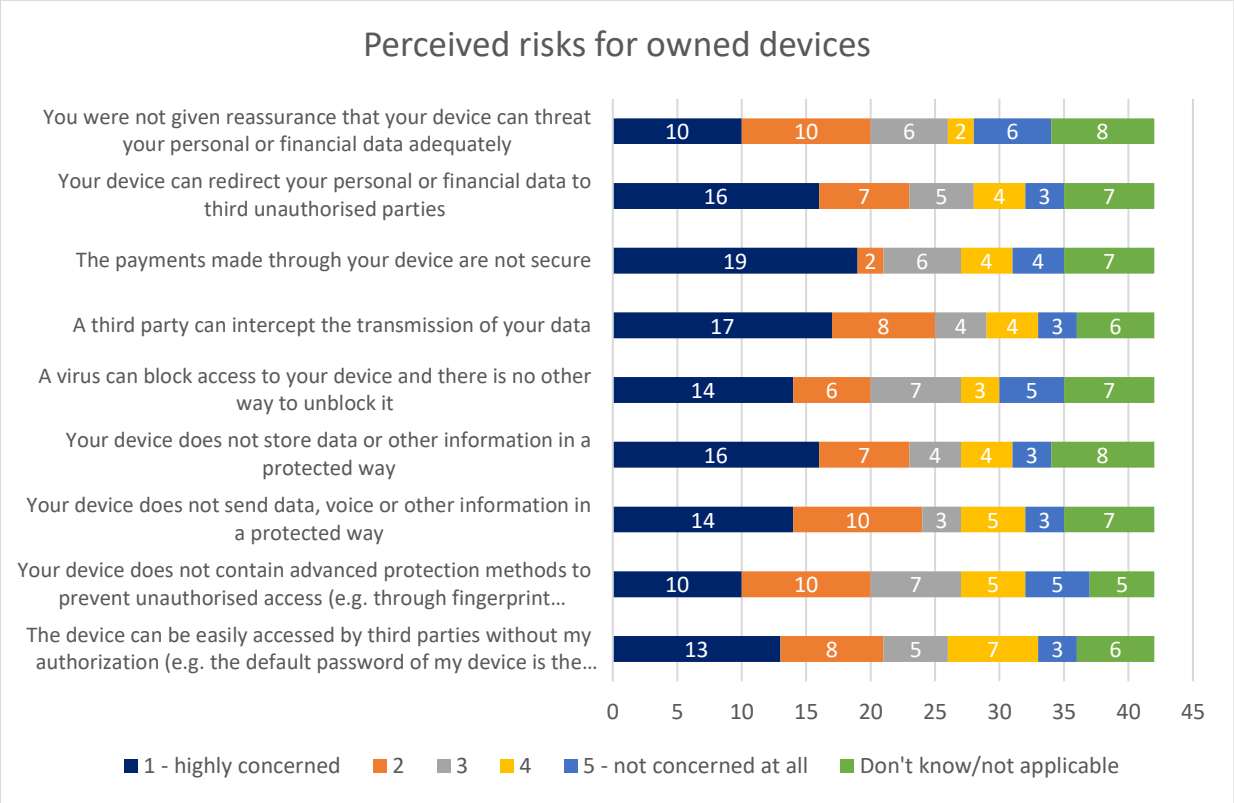
Currently there are no legal requirements regarding (i) data protection and privacy and (ii) protection from fraud that wireless connected devices and wearable devices have to fulfil as a condition for market access. Given this legal framework, respondents were asked to rate their level of concern about certain risks.

In respect of devices that they own:

- **All risks raised concern for the majority of respondents** (once "don't knows" are excluded), with at least 20 out of 42 respondents being highly (1/5) or fairly concerned (2/5);
- **Third party interception of data raised most concern**, with 25 respondents being highly or fairly concerned;
- **Lack of protection in the way that data, voice or other information is sent or stored were the next most common risks**, with 23-24 respondents being highly or fairly concerned;
- **Redirection of data to unauthorised third parties** was also of highly or fairly concerning to 23 respondents;
- **For each risk, few respondents had no concerns at all**, i.e. only 3-6 (7-14%).

[2] Firmware is permanent software programmed into a read-only memory.

Figure 9 Perceived risks for owned devices



Respondents were invited to identify other perceived risks or to elaborate on their replies. Their responses included the following:

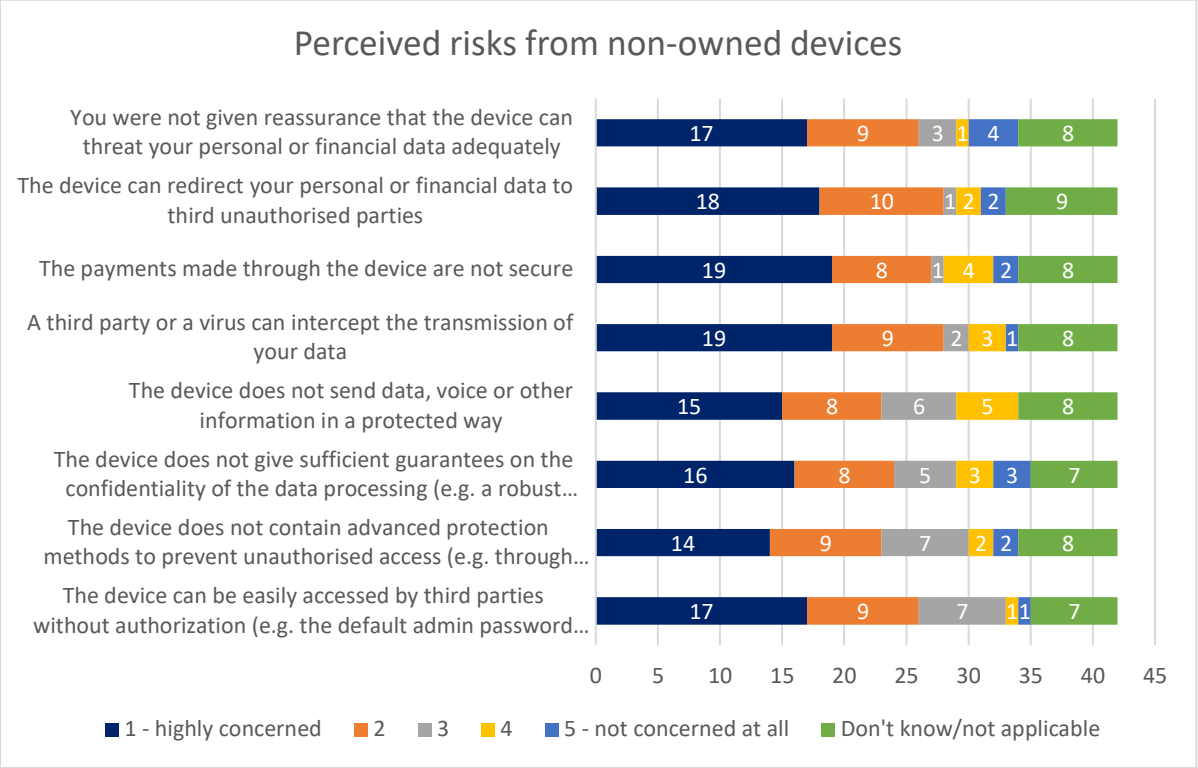
- Reliance on third parties to be diligent and ensure security of users' data;
- Failure by operators to inform users of data breaches in reasonable time so that they can take action;
- Communication of data to the state without users' consent (from a respondent in France);
- Lack of clarity within the GDPR over role of the operator in controlling and processing users' data and the separation between legitimate and illegitimate uses of data;
- Importance of manufacturers' own security measures.

In respect of devices that they do not own:

- **For all risks, respondents were more concerned about devices that they did not own** than about devices that they did own, i.e. in terms of being highly (1/5) or fairly concerned (2/5);
- **All risks raised concern for the majority of respondents** (once "don't knows" are excluded), with at least 23 out of 42 respondents being highly (1/5) or fairly concerned (2/5);
- **Third party interception of data raised most concern**, with 28 respondents being highly or fairly concerned;
- **Redirection of data to unauthorised third parties was also of most concern**, with 28 respondents being highly or fairly concerned;
- **Insecurity of payments mad through devices was the third most common risk**, with 23-24 respondents being highly or fairly concerned;

- **For each risk, very few respondents had no concerns at all**, i.e. only 1-4 (2-10%).

Figure 10 Perceived risks for non-owned devices



Respondents were invited to identify other perceived risks or to elaborate on their replies. Their responses included the following:

- Importance of operators using the full security capabilities of devices;
- Importance of public Wi-Fi having a high level of security and alerting users to potential risks;
- Importance of manufacturers' own security measures;
- Importance of operators' obligations under the GDPR;
- Lack of clarity within the GDPR over role of the operator in controlling and processing users' data and the separation between legitimate and illegitimate uses of data;
- Importance of the GDPR in required manufacturers or technology providers to support data controllers and processors to fulfil their obligations through data protection by design;
- Suggestion that a delegated act under RED promoters certification to ensure data protection by design, transparency, security measures and maintenance.

3.3 Issues experienced by users

3.3.1 Issues related to data protection and privacy

Respondents were asked to report whether they (or their family and friends) had experienced specific issues related to different types of devices in respect of data protection and privacy. Figure 11 shows that:

- **Each device had raised issues only for a minority of respondents** (even after exclusion of "don't know" responses);
- **Consumer devices with many functions (e.g. smartphones, laptops, smart TVs) had most often raised issues for respondents** (15 out of 33, after exclusion of "don't knows");
- **All other issues were experienced by no more than 17% of respondents** (or less, if "don't knows" are taken into account).

When asked about the severity of the issues experienced, **just over one-third (38%) reported that such issues had been extremely severe**. All but one of the other respondents had experienced issues that were marginally severe. (See Figure 12 and Figure 13). Of those who experienced problems, **most (62%) were deterred from buying or using such products again**, at least for some time (Figure 14).

Respondents were invited to describe the issues that they had experienced (via an open question).

These included issues related to **third party access to data**:

- Successful amateur penetration test exposing the vulnerabilities of an internet protocol camera;
- 3rd parties (potentially) listening to private conversations via wireless devices, e.g. baby monitor;
- Unknown devices trying to connect with smart televisions;
- Access to private email (no further explanation provided);
- Third party attempt to access company network and introduce viruses.

Some **issues related to the use of data gathered by devices**:

- Targeted advertising based on searches performed without giving consent;
- Receiving unwanted advertising on topics that had been discussed by smartphone (i.e. smartphone sending data from a private conversation, which generates targeted advertising);
- Manufacturer of a wearable device hesitating to release data when requested by the user.

Some **issues related to the design and operation of devices**:

- Pre-installed mobile applications impossible to eliminate and that collect health data;
- Privacy policies requiring users to consent to data being shared with 3rd parties outside the EU with no option to decline (other than not to use the device);
- Smartphone continuing to operate, even if software updates (required to ensure data protection and privacy) are not accepted by the user;
- Source code not disclosed (no further explanation provided).

Figure 11 Issues related to data protection and privacy

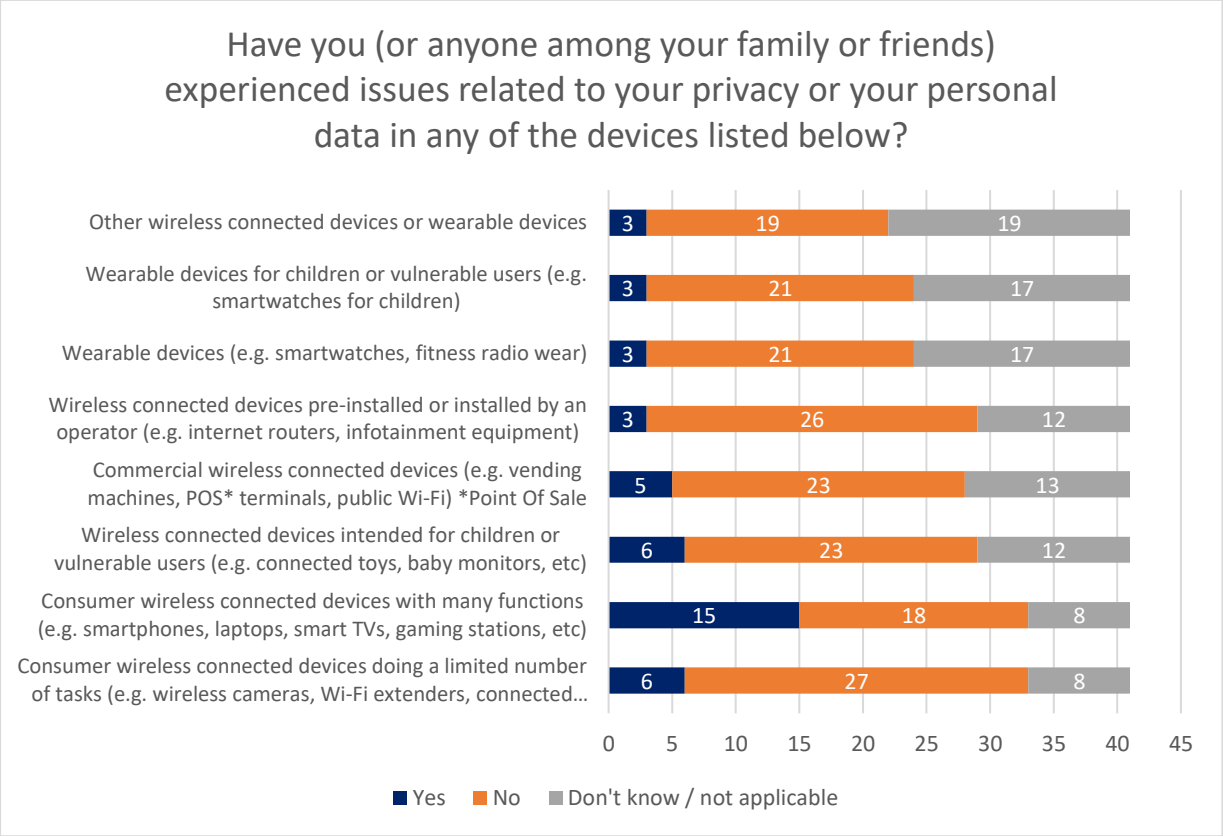


Figure 12 Severity of issues experienced (number of responses)

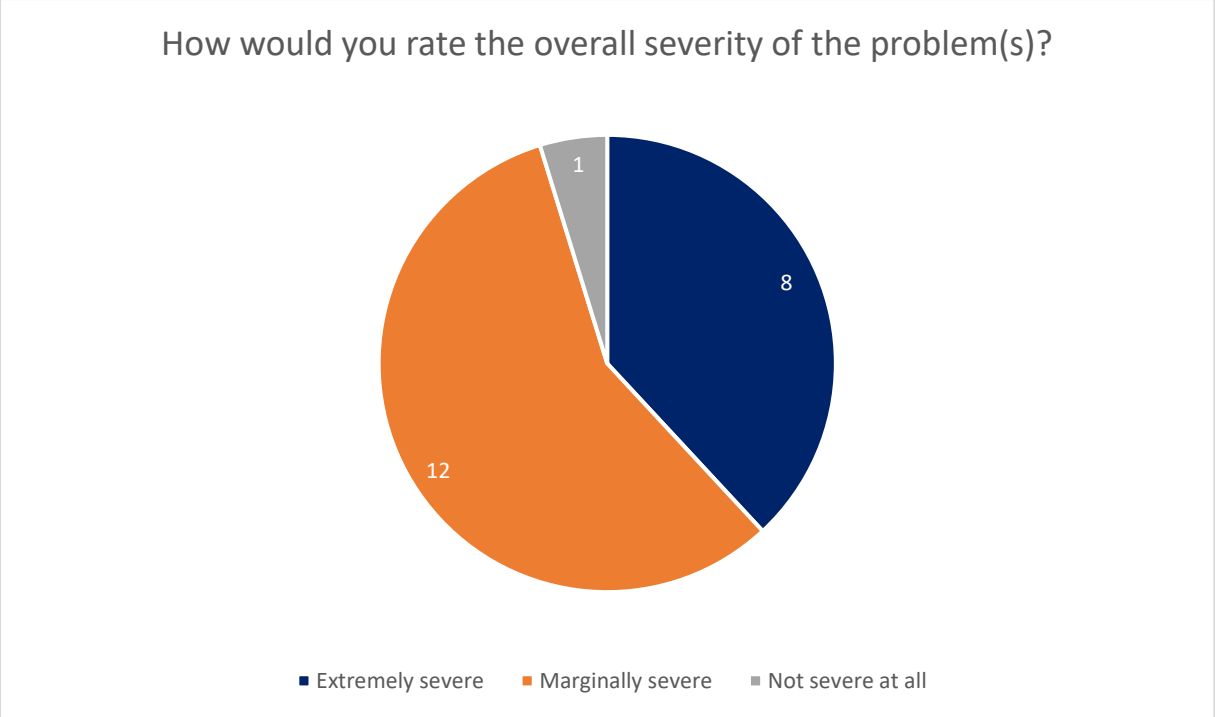


Figure 13 Severity of issues experienced (percentage of responses)

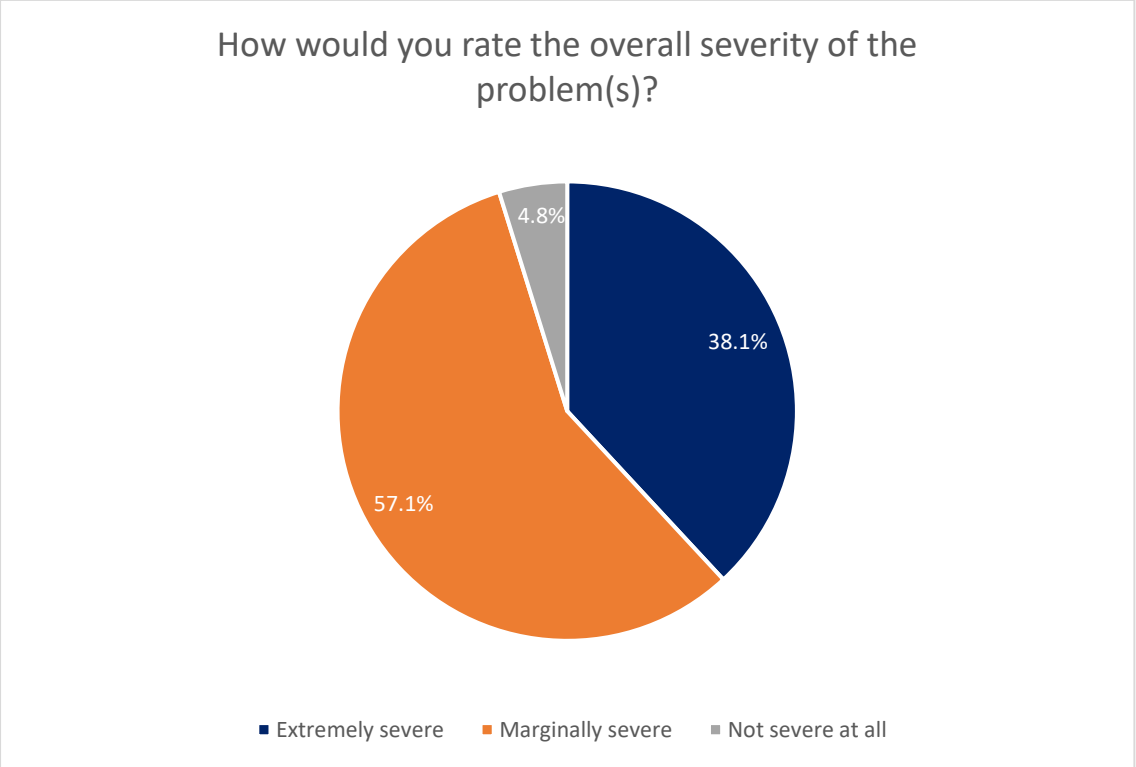


Figure 14 Deterrence effect of data protection problems experienced (number of responses)

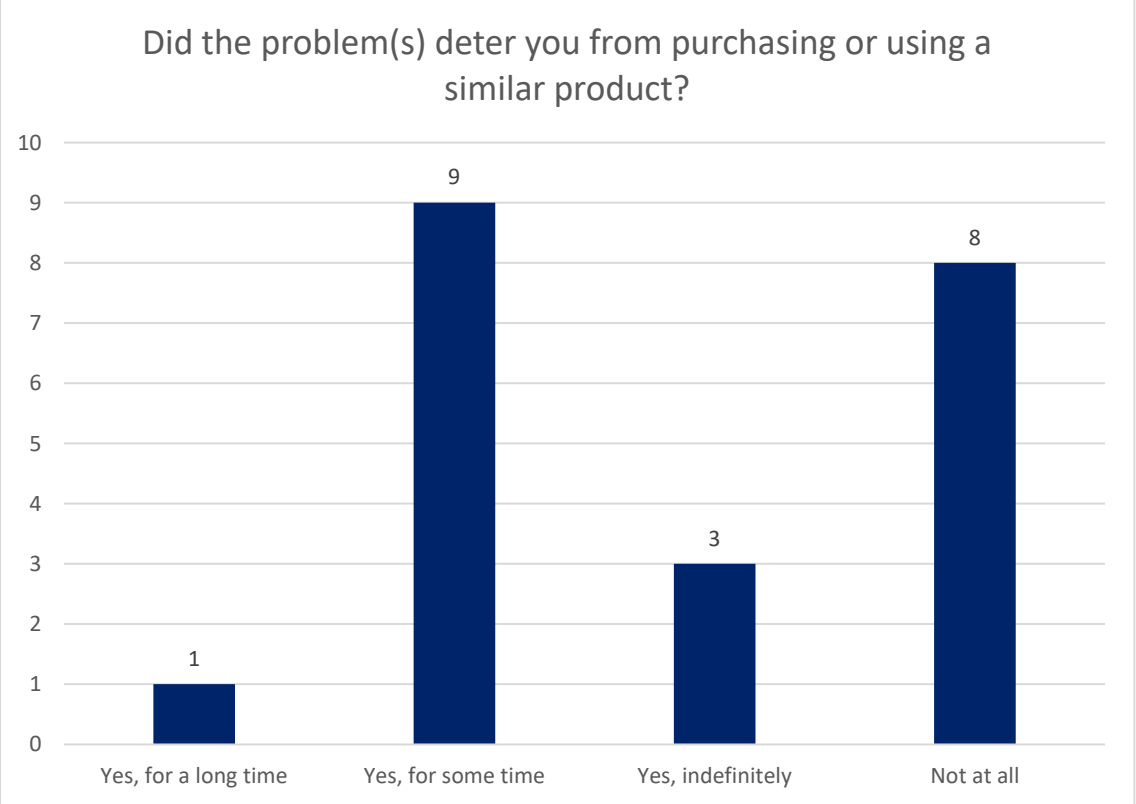
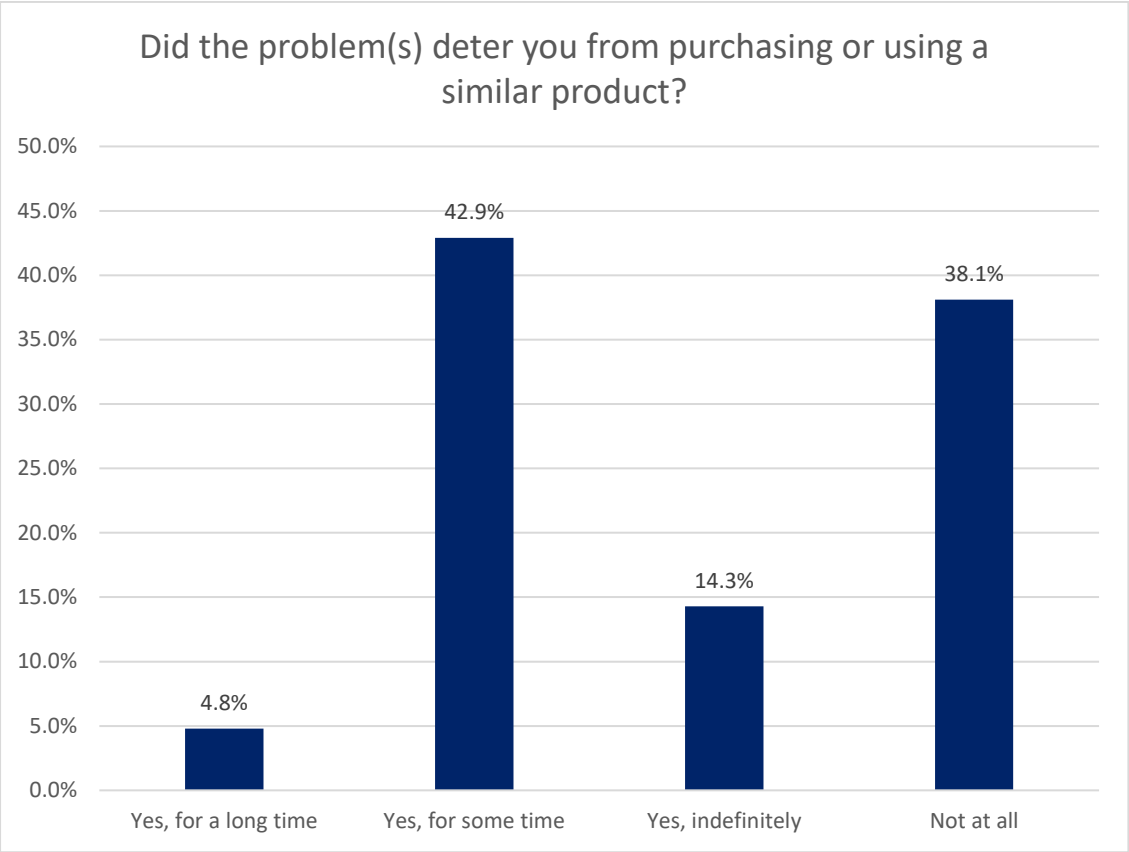


Figure 15 Deterrence effect of problems experienced (percentage of responses)



3.3.2 Issues related to protection from fraud

Respondents were asked to report whether they (or their family and friends) had been victims of fraud originating from the use of different types of devices. Figure 16, Figure 17 and Figure 18 show that:

- **Only 10% of respondents had been victims of fraud** (i.e. 10 out of 42);
- **Commercial devices and consumer devices with many functions were most commonly reported to have caused fraud**, i.e. for 6 out of 42 respondents;
- **Problems had been extremely severe for 3 out of the 10 respondents that had been victims of fraud**;
- **Of those experiencing fraud, 7 out of 10 were deterred from buying or using such products again**, at least for some time.

When asked to describe the problems experienced, two respondents gave examples of their bank cards being used for unauthorised transactions (i.e. by third-parties). For example, one related to a purchase made in a foreign country that the user had never visited. In both cases, the banks blocked the transactions or refunded the user, meaning that no losses were incurred.

Figure 16 Extent of fraud related to different types of device

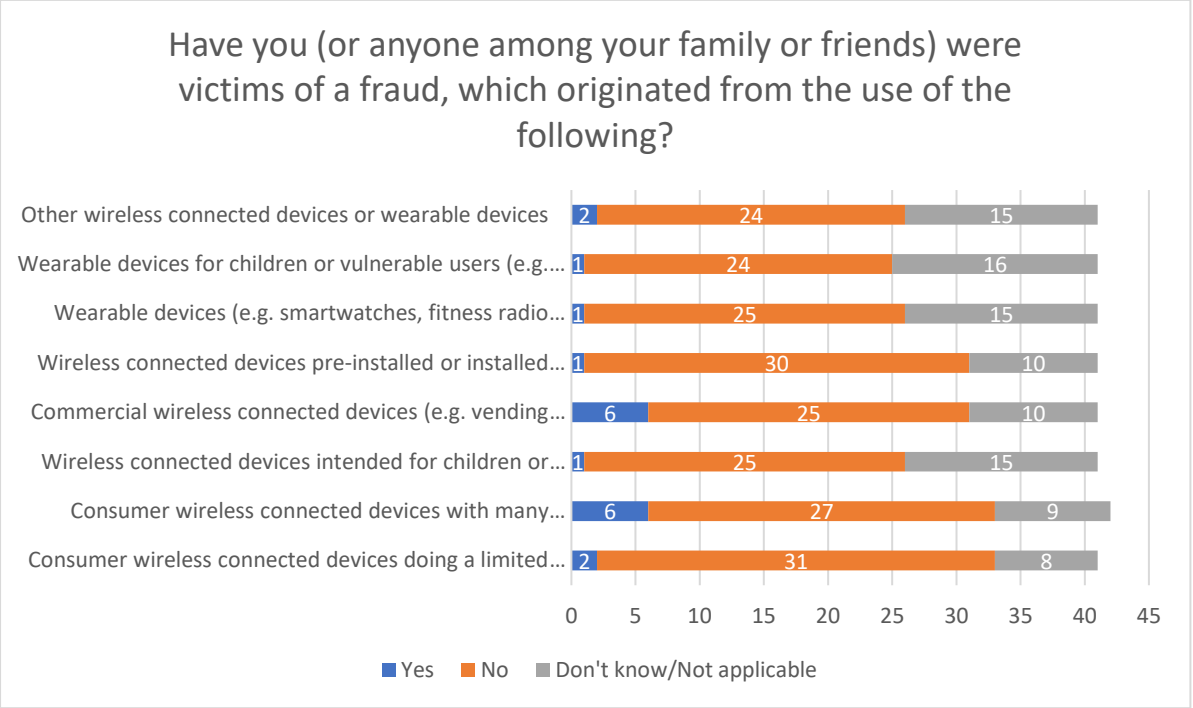


Figure 17 Severity of problems of fraud (number of respondents)

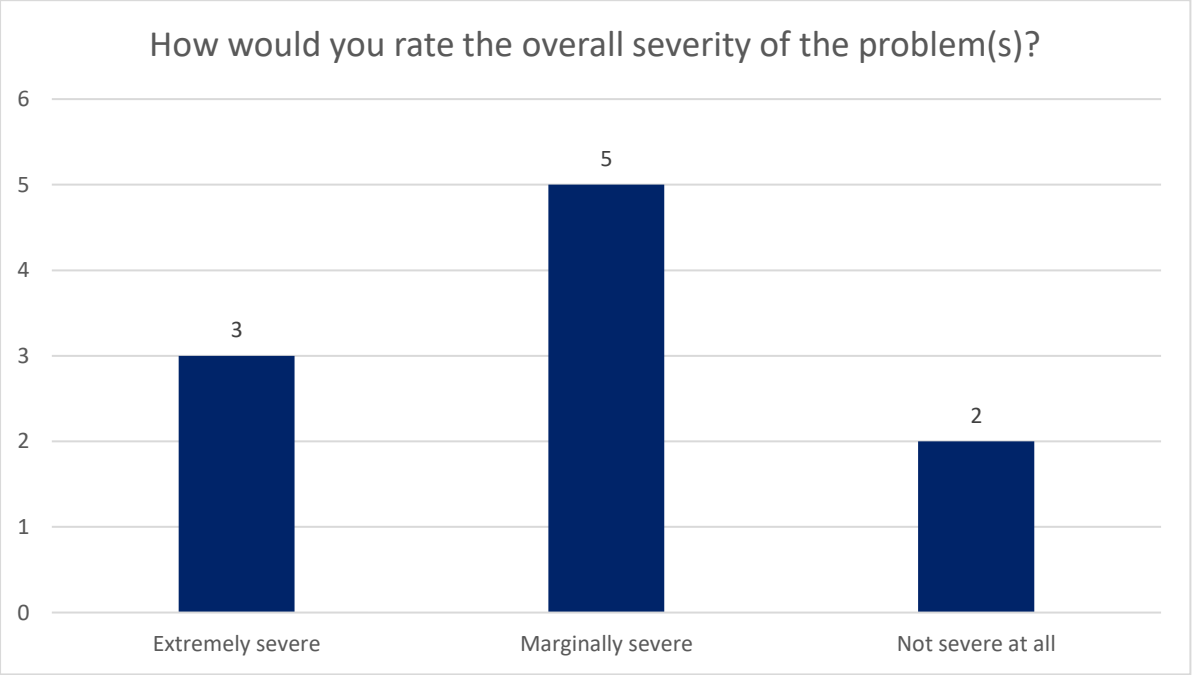
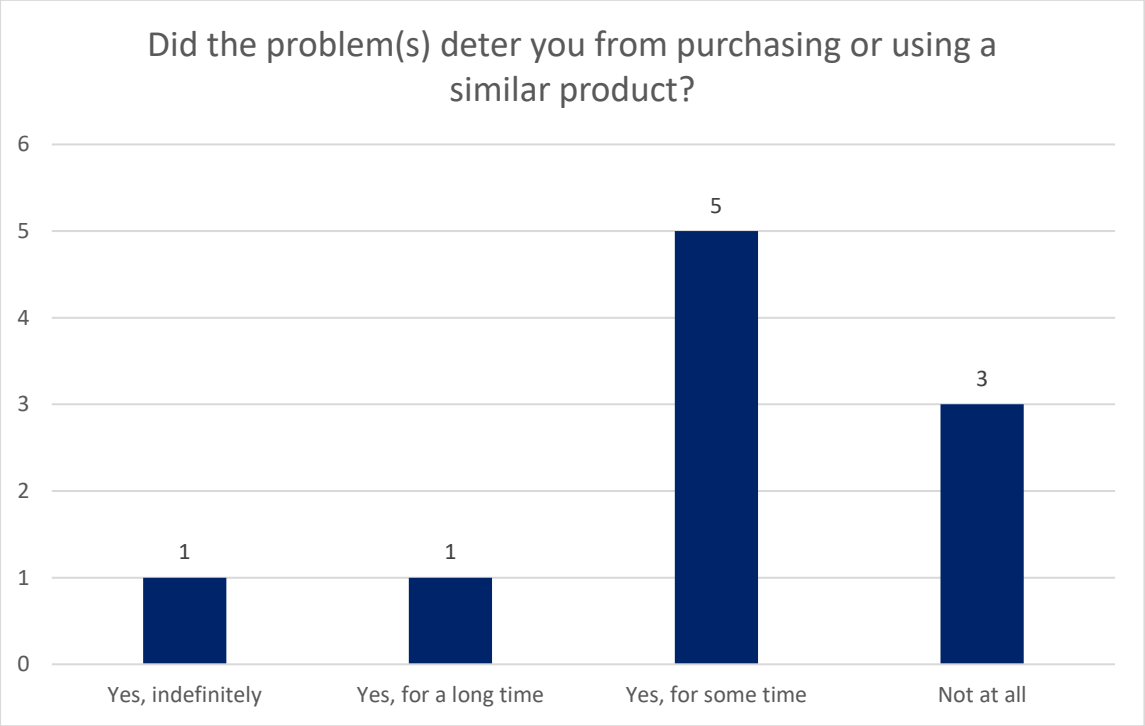


Figure 18 Deterrence effect of fraud problems experienced (number of responses)



4. Effects of new regulatory requirements

In line with the Better Regulation Guidelines, the OPC considered the impacts of the possible new regulatory requirements.

4.1 Perceived benefits of a regulatory approach

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

First, respondents were asked to consider where most benefit would arise in the event that manufacturers are asked to demonstrate that their products are adequate for the purposes of: i) data protection and privacy; and ii) protection from fraud.

As shown in Figure 19:

- **a majority of respondents expected each potential benefit to arise**;
- **the most commonly expected benefit was expected to come from manufacturers demonstrating that wireless connected devices have adequate privacy and data protection**.

When asked to comment on the potential benefits, respondents offered the following comments:

- two respondents reported that existing legislation was sufficient (one citizen and one business association);
- one business association (representing conformity assessment bodies and notified bodies) highlighted the importance of conformity assessment prior to placing products on the market and of market surveillance once products once products are on the market;
- one citizen suggested that strengthening regulatory requirements could give the EU a competitive advantage in global markets, given the growing international concern over protection of personal data.

Second, respondents were asked whether new regulatory protections would strengthen their trust in specific types of device. As shown in Figure 20:

- **A majority of respondents believed that new regulatory protections would increase trust in each type of device**;
- **New regulatory protections were most expected to be most effective in respect of "all wireless-connected and wearable devices with respect to protection from fraud" and in respect of "devices for children or vulnerable users with respect to data and privacy protection".**

One business association support the introduction of new regulatory requirements and recommended that the conformity assessment process should be strengthened. In its view, the process should consider the secure development life cycle process and particularly its vulnerability management process supported by functional security testing of the product. Manufacturers would thus have a way to patch and remediate future vulnerabilities as they are discovered. Conformity assessment bodies would need to test devices during use, receive anonymised raw data and source code from the manufacturer, and remain informed about changes to devices (e.g. software updates), so that they can assess their impact. A revision of the legislation would also require new guidance for policymakers, market surveillance authorities and manufacturers.

Figure 19 Potential benefits of new regulatory requirements

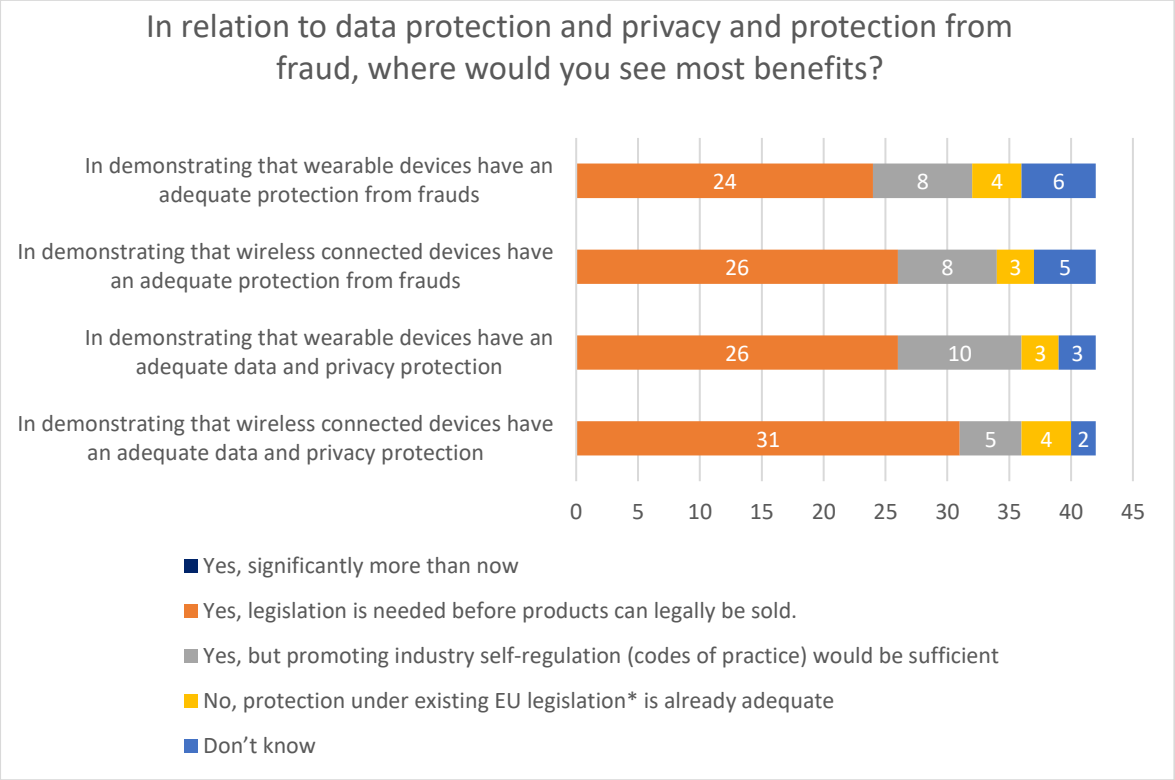
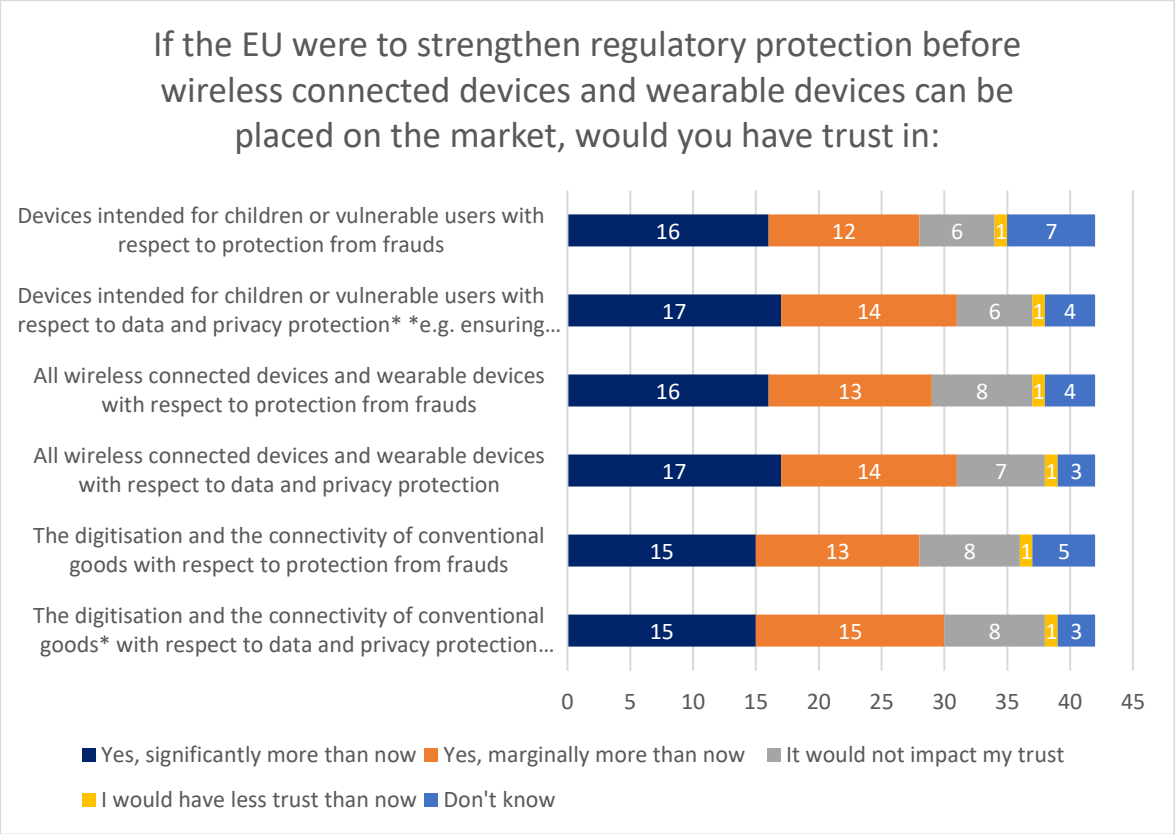


Figure 20 Potential to increase trust in specific types of device



4.2 Perceived disadvantages of a regulatory approach

The respondents were asked whether they believed there would be potential disadvantages in strengthening regulatory protection. As shown in Figure 21 and Figure 22:

- **There was a divergence of views**: just under half believed there would be disadvantages; just over a quarter believed there would not; and just over a quarter did not know;
- **There was no consensus within different types of respondent**, as shown in Table 1.

Table 1 Number of respondents perceiving disadvantages of a regulatory approach

Type of respondent	Yes	No	Don't know
Citizens	9	6	7
Companies, business organisations, business associations	6	4	3
Consumer associations	0	1	0
Public authorities	4	0	2
TOTALS	**19**	**11**	**12**

When asked to comment on their responses, the following disadvantages were mentioned:

- **additional cost and administrative burden** for manufacturers, which was mentioned by 8 respondents. As one respondent stated: "Strengthening the regulatory protection with a delegated act under the RED has the potential to create unnecessary burdens to our manufacturers, because sufficient measures are already in place and represent the "state of the art" in terms of technical solutions".
- **inhibition of innovation**. As one respondent stated: "Product development, market introduction and life cycle management (including legal disputes with customers, clients, authorities) would become more expensive, more complicated and would take longer".
- **unfair competition from non-EU manufacturers**, e.g. those who do not comply with new requirements. As one respondent stated: "It is questionable if non-European manufacturers (or manufacturers, importers, dealers with no intention to establish market presence and long-term business relationship with their costumers) will follow and finally comply with such legal requirements. If not, it can result in unfair competition".
- **unnecessary overlap or inconsistency with other EU legislation**, including the General Data Protection Regulation (GDPR)[3] or the Cybersecurity Act (CSA).[4] As, one respondent stated: "We believe it makes sense to strengthen regulatory protection on cybersecurity but we call for a horizontal approach to this, so that we have aligned requirements for various application areas such as RED, MD, LVD etc.".

[3] 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).
[4] 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).

In relation to this last point, several respondents suggested that the risks to data protection and privacy and protection from fraud needed to be addressed by "horizonal" legislation, rather than by product-specific legislation, such as the RED.

Linked to this, a concern expressed by several respondents was that EU legislation needed to address risks relating both to wireless and wired devices. This suggested a need for regulatory requirements to be introduced or strengthened through legislation other than the RED.

Figure 21 Potential disadvantages of new protections (number of respondents)

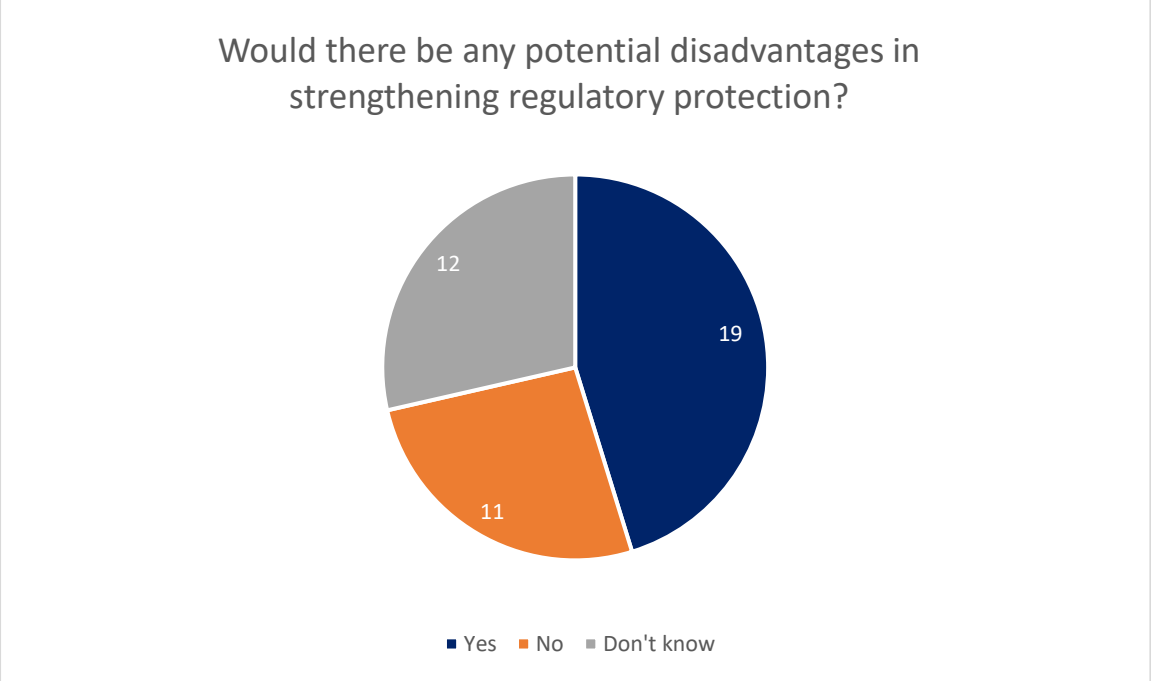


Figure 22 Potential disadvantages of new protections (percentage of respondents)