# ANEC replies to EC Study on the need of Cybersecurity Requirements for ICT Products

## Introduction

The long-lasting debate about the need of specific cybersecurity requirements for information and communications technology (ICT) products is mounting with the advent of the Internet of Things (IoT)[1]. In a scenario where "everything is connected with everything", an incident concerning ICT products can affect the whole system leading to severe impacts in terms of disruption to economic and social activities and ultimately threaten human life. The cybersecurity of such products is becoming all the more relevant and a solution that addresses market's needs but increases users' trust at the same time is necessary. At the same time, it appears that the existing EU regulatory framework might not be sufficient to tackle specifically the challenges linked to the security of connected products.

The European Commission, Directorate General for Communications Networks, Content & Technology (DG CNECT) has launched a "Study on the need of Cybersecurity Requirements for ICT Products – VIGIE 2020-0715". The study aims to explore the current state of cybersecurity in broad categories of ICT products, including non-embedded software, as well as to identify the reasons for inadequate security. Furthermore, the study shall provide a thorough analysis of the current regulatory landscape with regard to cybersecurity requirements for ICT products and explore options for an appropriate intervention by the policy makers for addressing the constantly rising cybersecurity risks in the use of the ICT products. The main study objectives are:

1. **Define the problem** by providing an overview of the current legislative framework for ICT products both at European and national level, by identifying the main problems, drivers, and consequences, linked to cybersecurity requirements for ICT products.
2. **Categorise ICT products and risk profiles** by defining an appropriate terminology for ICT products, developing and implementing a risk assessment methodology to identify the risk profiles inherent to each category of ICT products, and assessing how the identified categories of ICT products differ based on their use in specific sectors.
3. **Identify and recommend a set of cybersecurity requirements** specific to each risk profile.
4. **Propose a set of policy options** on the basis of the gap analysis of existing EU and national legislation, and the identified categories of ICT products and corresponding risk profiles.
5. **Assess the impact of each policy option** via an estimation of the likelihood and the magnitude of the impacts (i.e. economic, social and environmental) for each policy option.
6. **Formulate conclusions and recommendations** on the optimal way forward based on the assessment of impacts of the identified policy options.

The aim of this consultation is to allow stakeholders to express opinion on the results of the study. This consultation is open to everyone interested and willing to contribute. It would be particularly pertinent to National Competent Authorities in the area of cybersecurity, ICT industry and professional users of ICT

[1] The term IoT refers to a network of physical objects. These physical objects are devices or objects of different type and size, which are connected to the internet.

products, consumer associations and consumers of ICT products, and academic working in the field of cybersecurity.

The questionnaire is divided in the following sections:

- Problem definition.
- Categories of ICT products and risk profiles.
- Cybersecurity requirements for identified risk profiles.
- Identification of the policy options.
- Assessment of the possible impacts.

Written feedback provided in other document formats can be uploaded through the button made available at the end of the questionnaire.

The survey will remain open until 21 May 2021.

## General identification questions

**Q.1 Please provide your full name:**

*[Free Text]*

**Q.2 Email (this won't be published)***
*[Free Text]*

**Q.3 Please provide your affiliation:**

*[Select from the stakeholder types below] [Single choice]*

- **European Institution** (includes policymakers at the EU level (i.e. European Commission, other EU institutions and Agencies).
- **National Competent Authority** (includes Member State Competent Authorities (ministries or governmental bodies) with expertise in the implementation of EU legislation in the areas of product safety and cybersecurity (e.g. GPSD, Product Liability Directive, RED, CSA, GDPR, Machinery Directive, Medical Device Regulation); National accreditation bodies; Conformity assessment bodies (accredited by the Member States); National standardisation bodies; Market Surveillance Authorities (MSAs); all having responsibilities for the enforcement of the requirements of EU product safety and cybersecurity laws).
- **ICT industry** (includes ICT product developers and engineers; ICT device manufacturers; ICT maintenance and repair services).
- **Academic expert** (University professors; PhD students; Independent consultants specialised in the ICT industry).
- **Professional user** (Representatives of users in professional sectors that critically rely on ICT and that make use of sector-specific ICT products or services (e.g. banking, transport, energy,

manufacturing); Professional associations representing sectors impacted by the security of ICT products).

- **Consumer association and/or consumer** (Representatives of consumer organisations and citizens, consumers).
- **Other** (Any stakeholder that does not belong to any of the other categories).

*[If 'Other']* **Please specify:**

*[Free Text]*

**Q.4 Organisation name***
*[Free Text]*

**Transparency register number**
Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.
*[Free Text]*

**Q.5 Country of origin***
Please add your country of origin, or that of your organisation.
*[Single Choice][Select Box]*

**Q.6** * The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **For the purpose of transparency, the type of respondent (for example, 'business association, 'consumer association', 'EU citizen') country of origin, organisation name and size, and its transparency register number, are always published.** Your e-mail address will never be published. Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* **Publication privacy settings**
*[Select from the settings below][Single Choice]*

- **Anonymous** (Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous).
- **Public** (Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its country of origin and your contribution will be published. Your name will also be published).
- **Confidential (**Your organisation details and contribution will not be published. Only your type of respondent, and country of origin will be published).

* ☐ I agree with the personal data protection provision

# Problem definition

*[Background]*

The security of network and information systems represents an essential characteristic for the smooth functioning of the European Single Market in the digital era. While creating numerous opportunities for the European economy and society, the digitalisation of the single market brings forward several new challenges. As cyber-incidents and cyber-attacks generate the loss of billions of euros every year, cybersecurity, trust and privacy represent the foundations of a prosperous European Digital Single Market.

Nowadays an incident concerning ICT products can have severe consequences on the whole system both in terms of disruption to economic and social activities as well as threaten human life. Hence, the cybersecurity of ICT products is becoming of paramount importance to guarantee both increase trust of users in ICT products' users and for the overall smooth functioning of the Digital Single Market.

For the purpose of this study, an ICT product is defined as any good containing electronics or code within its structure, produced either for home/consumer or business/industrial purposes. An ICT product processes information and communication by electronic means, such as transmission and display, or uses electronic processing to detect, measure and/or record physical phenomena, or to control a physical process.

Furthermore, a *secure* ICT product is an ICT product that has embedded or implemented adequate cybersecurity measures in its design and development - aimed at limiting or preventing to the maximum extent possible cybersecurity vulnerabilities and avoiding cyber threats or risks that could harm the data protection or security of its users.

**Q1: In your opinion, what is the level of security of ICT products available across the EU?** [The ranking order is from number "1 = Poor", to number "5 = Excellent"].

- 1 Poor
- 2 Fair
- 3 Good
- 4 Very good
- 5 Excellent
- Do not know/no opinion

Please mention anything you would like to add: [Not compulsory and except for respondents answering 'Do not know/No opinion']

*As demonstrated by several of consumers organizations tests over the past years, many connected devices lack cybersecurity protection.*

**Q2: To what extent are the following statements a reason for inadequate security of ICT products across the EU?** [The ranking order is from number "1 = Strongly Disagree" that statement causes the lack of secure ICT products, to number "5 = Strongly Agree" with the stamen that causes the lack of secure ICT products].

| | 1. Strongly Disagree | 2. Somewhat Disagree | 3. Neither agree nor disagree | 4. Somewhat Agree | 5. Strongly Agree | Do not know / No opinion |
|---|---|---|---|---|---|---|
| No common legal basis that sets cybersecurity requirements for ICT products | ○ | ○ | ○ | ○ | ○X | ○ |
| No mandatory requirements (e.g. no clear obligations for the manufacturer) | ○ | ○ | ○ | ○ | ○X | ○ |
| No rules for post-market surveillance | ○ | ○ | ○ | ○ | ○X | ○ |
| No harmonised security by design principles at national level to increase the security of ICT products | ○ | ○ | ○ | ○ | ○ | ○X |
| No clear cybersecurity risk assessment model at EU level | ○ | ○ | ○X | ○ | ○ | ○ |
| No harmonised conformity assessment across the EU | ○ | ○ | ○ | ○ | ○X | ○ |
| Insufficient use of certifications by the manufacturers | ○ | ○ | ○X | ○ | ○ | ○ |
| No evident competitive advantages derived from cybersecurity | ○X | ○ | ○ | ○ | ○ | ○ |
| No incentives for manufacturers to make the products more secure | ○X | ○ | ○ | ○ | ○ | ○ |
| Cybersecurity not addressed in all stages of the product lifecycle (design, development, delivery, maintenance) | ○ | ○ | ○ | ○ | ○X | ○ |
| Cybersecurity of the ICT products has a high cost for the manufacturer | ○X | ○ | ○ | ○ | ○ | ○ |
| Manufacturers tend to care more for sales than security, | ○ | ○ | ○ | ○ | ○X | ○ |
| Low cooperation among Member States to define a common baseline for cybersecurity | ○ | ○ | ○X | ○ | ○ | ○ |
| Cybersecurity is considered a barrier rather than an enabler for the manufacturer | ○ | ○ | ○ | ○ | ○X | ○ |
| Cybersecurity requirements for ICT products differ across application domains | ○ | ○ | ○X | ○ | ○ | ○ |

| | 1. Strongly Disagree | 2. Somewhat Disagree | 3. Neither agree nor disagree | 4. Somewhat Agree | 5. Strongly Agree | Do not know / No opinion |
|---|---|---|---|---|---|---|
| Lack of qualified security professionals (i.e. developers) | ○ | ○ | ○ | ○ | ○ | ○x |
| Cybersecurity aspects not sufficiently covered in technical studies curricula | ○ | ○ | ○ | ○ | ○ | ○x |

Please mention anything you would like to add: [Not compulsory and except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q3 In your opinion, what is the level of understanding (awareness) among the professional users concerning the level of security of ICT products?** [The ranking order is from number "1 = Poor", to number "5 = Excellent"].

- 1 Poor
- 2 Fair
- 3 Good
- 4 Very good
- 5 Excellent
- Do not know/no opinion

Please mention anything you would like to add: [Not compulsory and except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q4 In your opinion, what is the level of understanding (awareness) among regular users (citizens) concerning the level of security of ICT products?** [The ranking order is from number "1 = Poor", to number "5 = Excellent"].

- 1 Poor
- 2 Fair
- 3 Good
- 4 Very good
- 5 Excellent
- Do not know/no opinion

Please mention anything you would like to add: [Not compulsory and except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q5 To what extent are the following statements a reason for insufficient understanding (lack of awareness/misperception) of the level of cybersecurity for ICT products among professional users ?**

[The ranking order is from number "1 = Strongly Disagree" that statement causes insufficient understanding among the users concerning the level of cybersecurity for ICT products, to number "5 = Strongly Agree" with the statement that causes the insufficient understanding among the users].

| | **1. Strongly Disagree** | **2. Somewhat Disagree** | **3. Neither agree nor disagree** | **4. Somewhat Agree** | **5. Strongly Agree** | **Do not know / No opinion** |
|---|---|---|---|---|---|---|
| No clear definition of the main requirements to ensure appropriate (and minimum) level of security of an ICT product | ○ | ○ | ○ | ○ | ○ | ○ |
| No available information for the cybersecurity properties of an ICT product | ○ | ○ | ○ | ○ | ○ | ○ |
| No methods to communicate the security level of an ICT product to the consumers | ○ | ○ | ○ | ○ | | ○ |
| Information asymmetry – the cybersecurity aspects of an ICT product are not visible and understandable by the buyer (e.g. market for lemons) | ○ | ○ | ○ | ○ | ○ | ○ |
| Security of an ICT product is expected by default | ○ | ○ | ○ | ○ | ○ | ○ |
| No common understanding between the manufacturer and the user of what a secure ICT product is | ○ | ○ | ○ | ○ | ○ | ○ |
| No skills required by users to use ICT products safely (e.g. passwords) | ○ | ○ | ○ | ○ | ○ | ○ |

Please mention anything you would like to add: [Not compulsory and except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q6 To what extent are the following statements a reason for insufficient understanding (lack of awareness/misperception) of the level of cybersecurity for ICT products among regular users (citizens)?**

[The ranking order is from number "1 = Strongly Disagree" that statement causes insufficient understanding among the users concerning the level of cybersecurity for ICT products, to number "5 = Strongly Agree" with the statement that causes the insufficient understanding among the users].

| | **1. Strongly Disagree** | **2. Somewhat Disagree** | **3. Neither agree nor disagree** | **4. Somewhat Agree** | **5. Strongly Agree** | **Do not know / No opinion** |
|---|---|---|---|---|---|---|
| No clear definition of the main requirements to ensure appropriate (and minimum) level of security of an ICT product | ○ | ○ | ○ | ○ | ○ | ○ |
| No available information for the cybersecurity properties of an ICT product | ○ | ○ | ○ | ○ | ○ | ○ |
| No methods to communicate the security level of an ICT product to the consumers | ○ | ○ | ○ | ○ | ○ | ○ |
| Information asymmetry – the cybersecurity aspects of an ICT product are not visible and understandable by the buyer (e.g. market for lemons) | ○ | ○ | ○ | ○ | ○ | ○ |
| Security of an ICT product is expected by default | ○ | ○ | ○ | ○ | ○ | ○ |
| No common understanding between the manufacturer and the user of what a secure ICT product is | ○ | ○ | ○ | ○ | ○ | ○ |
| No skills required by users to use ICT products safely (e.g. passwords) | ○ | ○ | ○ | ○ | ○ | ○ |

Please mention anything you would like to add: [Not compulsory and except for respondents answering 'Do not know/No opinion']

*Consumers should not bear the burden of cybersecurity and should be informed in an easy to understand way. Consideration shall be given to the legitimate expectations of consumers and the expected lifespan of the product (security updates).*

## Categories of ICT products and risk profiles

*[Background]*

The study presents a set of six generic ICT product categories (End devices, Software, Security, Programs for decision support, Networks, and Servers & systems) identified mainly through desk research. These categories are, as far as possible, linked to the five sectors covered in the study (Smart Manufacturing, Finance, Energy-Smart grid, Transport-Ports & Airports and Smart Home). The Project Team, in agreement

with DG CNECT, selected these indicative product categories and sectors on the basis of their good representativeness with regards to the cybersecurity of ICT products. The Project Team used an adapted risk assessment method to create risk profiles for each product category and sector, to enable a preliminary evaluation of risks, based on impact and likelihood. This work served as input for another study task related to policy options definition, especially on sector-specific policy options.

**Q7: Considering that an increasing number of products become smart/connected/IoT, please compare the five sectors covered by the study and rank them in terms of how severe cybersecurity threats they are currently facing** [The ranking order is from number 1 = highest relative threat level, to number 5 = lowest relative threat level]

| **Relative rank** / **Sector** | **1** (highest threat) | **2** | **3** | **4** | **5** (lowest threat) | Do not know / No opinion |
|---|---|---|---|---|---|---|
| **Smart Manufacturing** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Finance** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Energy (Smart Grid)** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Transport (ports and airports)** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Smart Home** | ○ | ○ | ○ | ○ | ○ | ○ |

Do you have anything to add?

*[Free Text]:*

## Cybersecurity requirements for identified risk profiles

*[Background]*

Essential Requirements are high-level requirements which are to be applied to a product (and to the services associated with a product, if and when their definition is aligned with the one from the Blue Guide of the European Union[2], with some specificities to keep in mind)[3]. Such requirements arise from certain hazards associated with the product *(for example physical and mechanical resistance, flammability, chemical, electrical or biological properties, hygiene, radioactivity, accuracy)*, or refer to the product or its performance (*for example provisions regarding materials, design, construction, manufacturing process, instructions drawn up by the manufacturer), or lay down the principal protection objective (for example by means of an illustrative list).* Often they are a combination of these.

[2] https://ec.europa.eu/growth/content/%E2%80%98blue-guide%E2%80%99-implementation-eu-product-rules-0_en

[3] One change in comparison to the New Legislative Framework is the application of Essential Requirements for the post market phase. While the NLF usually addresses manufacturers, importers and distributors, the defined Essential Requirements might involve a broader panel of stakeholders in the evaluation of product compliance (such as, but not limited to: maintainers, hardware providers, service providers, resellers, recyclers etc.).

The study identified specific cybersecurity essential requirements, as detailed below.

| # | Essential requirements | Description |
|---|---|---|
| ES1 | **Conceive the product to be secure by default and by design** | The requirement mandates the manufacturer to design and build the product securely so that the user can use it in a secure manner from the moment he/she purchases the product. |
| ES2 | **Address the threats of product compromising** | The requirement mandates the need to include in the product features and mechanisms, which protect the product from attackers and threats, and limit their ability to compromise the product. |
| ES3 | **Protect the identity and access of the user and product services** | The requirement mandates the need to ensure that the identity of the user and its associated access rights are protected on the product and on the services the product could use. |
| ES4 | **Protect the data and privacy of the user** | The requirement mandates the need to protect the data that the user could provide to the device, as well as to provide a high level of privacy on the user, as requested by the relevant legislation. |
| ES5 | **Raise the user's awareness to ensure a secure usage in his context** | The requirement mandates the need to support the user in its secure usage of the product, and to ease the configuration of the product throughout its lifecycle. |
| ES6 | **Ensure the resilience of the product and associated services** | The requirement mandates the need to provide the best level of availability of the services when it could be affected by incidents, and to limit the related impacts on the product's user. |
| ES7 | **Detect and react to security incidents** | The requirement mandates the need to identify threats weighting on the product and to respond to potential attacks through defense mechanisms. |
| ES8 | **Continuously evaluate and improve the security of the product** | The requirement mandates the need for the manufacturer to evaluate the security of the product throughout its lifecycle and to act upon risks and vulnerabilities identified. |

**Q8: In your opinion, what phase(s) of the ICT product lifecycle should the Essential Requirements target?**

- Before market placement
- After market placement
- Both
- I don't know, I have no opinion

Please justify your answer: [Except for respondents answering 'Do not know/No opinion']

*We do nor understand the use of the word 'mandates' in the requirements as we think it should be 'oblige/make mandatory'.*

**Q9: To what extent do Essential Requirements listed above address the main cybersecurity risks faced by ICT products?** [The ranking order is from number 1 = do not address the main cybersecurity risks, to number 5 = address completely the main cybersecurity risks]

| | | 1. Do not address the main cybersecurity risks | 2. | 3. | 4. | 5. Address completely the main cybersecurity risks | Do not know / No opinion |
|---|---|---|---|---|---|---|---|
| ES1 | **Conceive the product to be secure by default and by design** | ○ | ○ | ○ | ○ | ○ | ○ |
| ES2 | **Address the threats of product compromising** | ○ | ○ | ○ | ○ | ○ | ○ |
| ES3 | **Protect the identity and access of the user and product services** | ○ | ○ | ○ | ○ | ○ | ○ |
| ES4 | **Protect the data and privacy of the user** | ○ | ○ | ○ | ○ | ○ | ○ |
| ES5 | **Raise the user's awareness to ensure a secure usage in his context** | ○ | ○ | ○ | ○ | ○ | ○ |
| ES6 | **Ensure the resilience of the product and associated services** | ○ | ○ | ○ | ○ | ○ | ○ |
| ES7 | **Detect and react to security incidents** | ○ | ○ | ○ | ○ | ○ | ○ |
| ES8 | **Continuously evaluate and improve the security of the product** | ○ | ○ | ○ | ○ | ○ | ○ |

Please briefly explain your answer: [Except for respondents answering 'Do not know/No opinion']

*We have elaborated a list of requirements from a consumer point of view (available on request). A distinction should be made between technical and organisational requirements.*

# Identification of the policy options

*[Background on Policy Options]*

As mentioned in the introduction, one of the goals of this study is to explore options for an appropriate intervention by the policy makers for addressing the constantly rising cybersecurity risks in the use of ICT products. In this context, the project team of this study identified several potential policy options.

These policy options have been designed following the terms of references of the study, desk research, interviews with Members States policy makers, industry and consumer organizations and competent authorities.

At a glance, the policy options are defined for the purpose of this study as follows:

| **Policy option 0: Baseline** | **Policy Option 1: Voluntary Measures** | **Policy Option 2: Horizontal Legislation** | **Policy Option 3: Sector Specific Legislation** | **Policy Option 4: Mixed Approach** |
|---|---|---|---|---|
| Do Nothing. This policy option entails leaving the current situation as it is now: no additional legislative actions, no additional initiatives to contrast the increasing cybersecurity threats for ICT products: overall "no policy change scenario". | Current voluntary practices and measures to increase transparency and promote conformity assessment | Implementation of a common regulatory approach applicable to all categories and risk profile of ICT products | Implementation of a common regulatory approach applicable only to specific ICT Product / risk levels or sector | Implementation of a combination of regulatory and voluntary measures |

The following sections will briefly explain the content of each policy options. Your answers will be relevant for the choice of the preferred option.

*[Background before Q8]*

**Policy Option 1: Voluntary measures**

This option include the following voluntary practices and measures to increase transparency and promote conformity assessment:

| | |
|---|---|
| **Voluntary Certification as defined in the Cybersecurity Act** | Conformity assessment for evaluating whether specified requirements relating to an ICT product, services or process have been fulfilled (Examples: IoT Labelling in Finland, IT Security Label in Germany, EU-CC, Cloud Services schemes,<br>Certification scheme for IoT*). |
| **Code of Conducts** | Policy makers can promote codes of conducts, voluntary frameworks and guidance to support supply-side stakeholders to enhance digital security of their products (Examples: UK The code of Practice for Consumer IoT, IoT Security Safety Framework in Japan, NIST Framework of 2018 and the IoT Device Cybersecurity Capability Core baseline in 2020). |
| **Government procurement policy** | Governments can require ICT suppliers operating within their jurisdiction to comply with certain security, privacy, or related requirements (Examples: Scottish Cyber Assessment Service and the Supplier Cybersecurity Guidance note, Cybersecurity Maturity Model Certification (CMMC) in the USA). |
| **Awareness raising campaigns** | Increasing awareness on the security of ICT products through media campaign and ad hoc training in schools and universities (Examples: European Commission Cybersecurity month (ECSM), Do your update and against fishing campaigns in the Netherlands, German government is planning IoT security campaign for consumers). |
| **Commission Recommendations** | |
| **Industry-led initiatives** | |

**Q10: To what extent does the adoption of voluntary measures address the need of cybersecurity of ICT products?** [The ranking order is from number 1 = do not address the cybersecurity of ICT products, to number 5 = address completely the cybersecurity of ICT products]

- 1
- 2
- 3
- 4
- 5
- I don't know, I have no opinion

Please briefly explain your answer: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q11: Which of the following policy measures, envisaged under Policy Option 1- Voluntary Measures, is more relevant to address the need of cybersecurity for ICT products?**

| | Significantly relevant | Moderately relevant | Barely relevant | Not relevant at All | Do not know / No opinion |
|---|---|---|---|---|---|
| Voluntary Certification as defined in the Cybersecurity Act | o | o | o | o | o |
| Codes of Conduct | o | o | o | o | o |
| Government procurement policy | o | o | o | o | o |
| Awareness-raising campaigns | o | o | o | o | o |
| Commission Recommendations | o | o | o | o | o |
| Industry-led initiatives | o | o | o | o | o |

Please briefly explain your answer. Please complement with any further policy measures missing from the list: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q12: Please briefly explain any possible effects, negative or positive, stemming from the implementation of voluntary measures.**

*[Free Text]*

*[Background text before Q10]*

**Policy Option 2: Horizontal legislation**

This option would include the implementation of a common regulatory approach applicable to all categories and risk profiles of ICT products, and would be based on the following policy measures:

| | |
|---|---|
| **Essential Requirements** | The essential requirements are high-level requirements for ICT products and are not technology-specific and should in principle be applicable to broad categories of products. Requirements may apply to the product itself (e.g., the product should have certain features) or to processes related to the design, development, delivering or maintaining of the product. |
| **Conformity Assessment** | Conformity assessment procedures/methods define how compliance to requirements is assessed. The Study Project Team has identified a set of applicable conformity assessment methods that apply both ex-ante and ex-post to ensure that the security of the product once placed on the market is also assessed. |

| | |
|---|---|
| | Conformity assessment could be carried out by the manufacturer/vendor or a third party depending amongst others on the risk involved and possible the nature of the product and intended use.<br><br>Non-Mandatory/ mandatory involvement of notified bodies. |
| **Market surveillance** | In the context of Cybersecurity for ICT products, beside the current rules for market surveillance envisaged by the NLF, since it is required to guarantee security through the entire lifecycle of the products it is necessary to extend the post-market surveillance activity to guarantee the security of product during the usage phase and when the products are removed from the market:<br><br>• Sharing and dissemination of cybersecurity information and knowledge of cybersecurity vulnerabilities and threats across multiple sectors<br>• Vulnerability remediation<br>• Incident response<br>• Product phasing out<br>• Production of Post Market Surveillance (PMS) Plan and Post market Reports (PMSRs)<br>• Auditing |

**Q13: To what extent could the establishment of a horizontal legislation for ICT products and services address the need of cybersecurity of ICT products?** [The ranking order is from number 1 = do not address the cybersecurity of ICT products, to number 5 = address completely the cybersecurity of ICT products]

- 1
- 2
- 3
- 4
- 5
- I don't know, I have no opinion

Please briefly explain your answer: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q14: To what extent do you agree with the following statements: The horizontal legislation would result in:**

| | **1. Strongly Disagree** | **2. Somewhat Disagree** | **3. Neither agree nor disagree** | **4. Somewhat Agree** | **5. Strongly Agree** | **Do not know / No opinion** |
|---|---|---|---|---|---|---|
| **Greater security** | ○ | ○ | ○ | ○ | ○ | ○ |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Regulatory certainty** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced liability for companies** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced Innovation** | ○ | ○ | ○ | ○ | | ○ |
| **Race to the bottom** | ○ | ○ | ○ | ○ | | ○ |

Please briefly explain your answer. Please complement with any further possible effects stemming from the implementation of a horizontal legislation missing from the list: [Except for respondents answering 'Do not know/No opinion']

*The role of Harmonised Standards, providing presumption of conformity with the relevant legislation, should also be stressed. In combination with a risk-based approach, tailored solutions for a wide range of product areas and safety requirements can be developed in a cost-effective and efficient way.*

*[Background text before Q13]*

**Policy Option 3: Sector Specific legislation**

Alternatively to the already presented horizontal legislation, which is characterized by a very broad scope entailing a set of requirements applied to all sectors and categories of products, a more targeted approach should also be considered.

This would be the case of the **sector specific legislation** approach: **the implementation of a common regulatory approach applicable only to specific ICT Product / risk levels or sectors.** It means that, the basic regulatory measures envisaged for the horizontal legislation (essential requirements, conformity assessment, life cycle, market surveillance) will still characterize the sector specific legislation policy option but this time will be applied only to specific ICT products/risk level or sectors. .

This policy option, in particular, might consist of three types:

- **Type 1**: Implementation of a common regulatory approach applicable only to specific ICT product categories (Ex: End devices).
- **Type 2**: Implementation of a common regulatory approach applicable only to specific risk levels of ICT products categories (Ex: essential and/or high risk).
- **Type 3**: Implementation of a common regulatory approach applicable only to a specific intended use or sector (Ex: Consumer products /Smart Homes).

| | | **Type 1** | **Type 2** | **Type 3** |
|---|---|---|---|---|
| **Risk Profiles** | *All* | ✓ | | ✓ |
| | *Some* | | ✓ | |

| | | | | |
|---|---|---|---|---|
| **Product/Sector Categories** | *All* | | ✓ | |
| | *Some* | ✓ | | ✓ |
| **Life-Cycle Approach** | | ✓ | ✓ | ✓ |
| **Essential Requirements** | | ✓ | ✓ | ✓ |
| **Conformity Assessment** | | ✓ | ✓ | ✓ |
| **Market Surveillance** | | ✓ | ✓ | ✓ |

**Q15: To what extent could the establishment of sector-specific legislation per sector address the need of cybersecurity of ICT products overall?** [The ranking order is from number 1 = do not address the cybersecurity of ICT products, to number 5 = address completely the cybersecurity of ICT products]

- 1
- 2
- 3
- 4
- 5
- I don't know, I have no opinion

Please briefly explain your answer: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q16: Which of the following Sector-Specific Legislation types would be the most relevant to address the need of cybersecurity of ICT products?**

| | Significantly relevant | Moderately relevant | Barely relevant | Not relevant at All | Do not know / No opinion |
|---|---|---|---|---|---|
| Implementation of a common regulatory approach applicable only to specific ICT product categories (Ex: End-devices) | o | o | o | o | o |
| Implementation of a common regulatory approach applicable only to specific risk levels of ICT products categories (EX: essential and/or high) | o | o | o | o | o |

| | | | | | |
|---|---|---|---|---|---|
| Government procurement policy Implementation of a common regulatory approach applicable only to a specific intended use or sector (Ex: Consumer products/Smart Homes) | ○ | ○ | ○ | ○ | ○ |

Please briefly explain your answer. Please complement with any further sector specific types missing from the list: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q17: To what extent do you agree with the following statements: the sector specific legislation of type 1 (implementation of a common regulatory approach applicable only to specific ICT product categories (Ex: end devices)) would result in:**

| | 1. Strongly Disagree | 2. Somewhat Disagree | 3. Neither agree nor disagree | 4. Somewhat Agree | 5. Strongly Agree | Do not know / No opinion |
|---|---|---|---|---|---|---|
| **Greater security** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Regulatory certainty** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced liability for companies** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced Innovation** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Race to the bottom** | ○ | ○ | ○ | ○ | ○ | ○ |

Please briefly explain your answer. Please complement with any further possible effects stemming from the implementation of sector specific legislation of type 1 missing from the list: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q18: To what extent do you agree with the following statements: the sector specific legislation of type 2 (implementation of a common regulatory approach applicable only to specific risk levels of ICT products categories (Ex: essential and/or high risk)) would result in:**

| | 1. Strongly Disagree | 2. Somewhat Disagree | 3. Neither agree nor disagree | 4. Somewhat Agree | 5. Strongly Agree | Do not know / No opinion |
|---|---|---|---|---|---|---|
| **Greater security** | ○ | ○ | ○ | ○ | ○ | ○ |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Regulatory certainty** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced liability for companies** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced Innovation** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Race to the bottom** | ○ | ○ | ○ | ○ | ○ | ○ |

Please briefly explain your answer. Please complement with any further possible effects stemming from the implementation of a sector specific legislation of type 2 missing from the list: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q19: To what extent do you agree with the following statements: the sector specific legislation of type 3 (Implementation of a common regulatory approach applicable only to a specific intended use or sector (Ex: consumer products /smart Homes)) would result in:**

| | 1. Strongly Disagree | 2. Somewhat Disagree | 3. Neither agree nor disagree | 4. Somewhat Agree | 5. Strongly Agree | Do not know / No opinion |
|---|---|---|---|---|---|---|
| **Greater security** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Regulatory certainty** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced liability for companies** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced Innovation** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Race to the bottom** | ○ | ○ | ○ | ○ | ○ | ○ |

Please briefly explain your answer. Please complement with any further possible effects stemming from the implementation of a sector specific legislation of type 3 missing from the list: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

*[Background for Q15]*

**Policy option 4: Mixed approach (regulatory + voluntary measures)**

Furthermore, to allow for more flexibility and fit ad hoc situations an additional policy option could be envisaged: **the mixed approach**. This option would involve the implementation of a **combination of regulatory and voluntary measures**. For instance, this option could mandate a set of minimum requirements for some products and suggest a labelling system for some others. This policy option might consist of two types:

- **Type 1**: Implementation of a combination of regulatory and voluntary measures applicable to all categories and risk profiles of ICT products.

- **Type 2**: Implementation of a combination of regulatory and voluntary measures applicable only to a specific intended use or sector (Ex: Smart Homes).

| | | **Type 1** | **Type 2** |
|---|---|---|---|
| **Risk Profiles** | *All* | ✓ | ✓ |
| **Product/Sector Categories** | *All* | ✓ | |
| | *Some* | | ✓ |
| **Life-Cycle Approach** | | ✓ | ✓ |
| **Essential Requirements** | | ✓ | ✓ |
| **Conformity Assessment** | | ✓ | ✓ |
| **Market Surveillance** | | ✓ | ✓ |

**Q20: To what extent could the establishment of a Mixed Approach address the need of cybersecurity of ICT products?** [The ranking order is from number 1 = do not address the cybersecurity of ICT products, to number 5 = address completely the cybersecurity of ICT products]

- 1
- 2
- 3
- 4
- 5
- I don't know, I have no opinion

Please briefly explain your answer: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q21: To what extent would the following mixed approach types be relevant to address the need of cybersecurity of ICT products?**

| | Significantly relevant | Moderately relevant | Barely relevant | Not relevant at all | Do not know / No opinion |
|---|---|---|---|---|---|
| Implementation of a combination of common regulatory approach (a limited set of requirements) applicable to all categories and risk profiles of ICT products + voluntary measures | ○ | ○ | ○ | ○ | ○ |
| Implementation of a combination of common regulatory approach (a limited set of requirements) applicable only to a specific intended use or sector (Ex: Smart Homes) + voluntary measures | ○ | ○ | ○ | ○ | ○ |

Please briefly explain your answer: Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q22: To what extent do you agree with the following statements: the mixed approach of type 1 (implementation of a combination of regulatory and voluntary measures applicable to all categories and risk profiles of ICT products) would result in:**

| | 1. Strongly Disagree | 2. Somewhat Disagree | 3. Neither agree nor disagree | 4. Somewhat Agree | 5. Strongly Agree | Do not know / No opinion |
|---|---|---|---|---|---|---|
| **Greater security** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Regulatory certainty** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced liability for companies** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced Innovation** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Race to the bottom** | ○ | ○ | ○ | ○ | ○ | ○ |

Please briefly explain your answer. Please complement with any further possible effects stemming from the implementation of a mixed approach of type 1 missing from the list: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q23: To what extent do you agree with the following statements: the mixed approach of type 2 (implementation of a combination of regulatory and voluntary measures applicable only to a specific intended use or sector (Ex: Smart Homes) would result in:**

| | 1. Strongly Disagree | 2. Somewhat Disagree | 3. Neither agree nor disagree | 4. Somewhat Agree | 5. Strongly Agree | Do not know / No opinion |
|---|---|---|---|---|---|---|
| **Greater security** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Regulatory certainty** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced liability for companies** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Reduced Innovation** | ○ | ○ | ○ | ○ | ○ | ○ |
| **Race to the bottom** | ○ | ○ | ○ | ○ | ○ | ○ |

Please briefly explain your answer. Please complement with any further possible effects stemming from the implementation of a mixed approach of type 2 missing from the list: [Except for respondents answering 'Do not know/No opinion']

*[Free Text]*

**Q24: Which of the proposed Policy Option would address better the need for cybersecurity requirements for ICT products?**

- Policy Option 0 – Baseline/Do Nothing
- Policy Option 1 – Voluntary Measures
- Policy Option 2 – Horizontal Approach
- Policy Option 3 – Sector-Specific Legislation
- Policy Option 4 – Mixed Approach
- Don't know / No opinion

Please briefly explain your answer: [Except for respondents answering 'Do not know/No opinion']

Regulations concerning consumer safety should always be introduced as horizontal legislation. The best example of this is the GPSD. An analogous approach should therefore also be sought for the area of cybersecurity. Whether it makes sense to expand the GPSD to include cybersecurity or to create a separate directive remains to be discussed. In view of the increasing digitization of consumer products, there is a good rationale for integration.

## Assessment of the possible impacts

**Q25: In your opinion, what would be the impact on costs of the Policy Option 1: Voluntary measures in comparison to no policy action?**

| | High increase in costs | Small increase in costs | No change | Small decrease in costs | High decrease in costs | Don't know / No answer |
|---|---|---|---|---|---|---|
| Administrative burden for Public administrations (local/regional/national) | | | | | | x |
| Compliance costs for Business (ICT products producers and professional users) | | | | | | x |
| Monitoring and enforcement costs for National Competent Authorities | | | | | | x |
| Charges for consumers/citizens | | | | | | x |
| Other costs | | | | | | x |

Could you provide an indication of costs, if possible, in FTE/EUR?

*[Free Text]*

**Q26: In your opinion, what would be the impact on costs of the Policy Option 2: Horizontal legislation in comparison to no policy action?**

| | High increase in costs | Small increase in costs | No change | Small decrease in costs | High decrease in costs | Don't know / No answer |
|---|---|---|---|---|---|---|
| Administrative burden for Public administrations (local/regional/national) | | | | | | x |
| Compliance costs for Business (ICT products producers and professional users) | | | | | | x |
| Monitoring and enforcement costs for National Competent Authorities | | | | | | x |
| Charges for consumers/citizens | | | | | | x |
| Other costs | | | | | | x |

Could you provide an indication of costs, if possible, in FTE/EUR?

*[Free Text]*

**Q27: In your opinion, what would be the impact on costs of the Policy Option 3: Sector Specific legislation in comparison to no policy action?**

| | High increase in costs | Small increase in costs | No change | Small decrease in costs | High decrease in costs | Don't know / No answer |
|---|---|---|---|---|---|---|
| Administrative burden for Public administrations (local/regional/national) | | | | | | x |
| Compliance costs for Business (ICT products producers and professional users) | | | | | | x |
| Monitoring and enforcement costs for National Competent Authorities | | | | | | x |
| Charges for consumers/citizens | | | | | | x |
| Other costs | | | | | | x |

Could you provide an indication of costs, if possible, in FTE/EUR?

*[Free Text]*

**Q28: In your opinion, what would be the impact on costs of the Policy Option 4: Mixed approach (regulatory + voluntary measures) in comparison to no policy action?**

| | High increase in costs | Small increase in costs | No change | Small decrease in costs | High decrease in costs | Don't know / No answer |
|---|---|---|---|---|---|---|
| Administrative burden for Public administrations (local/regional/national) | | | | | | x |
| Compliance costs for Business (ICT products producers and professional users) | | | | | | x |
| Monitoring and enforcement costs for National Competent Authorities | | | | | | x |
| Charges for consumers/citizens | | | | | | x |

| | | | | | | |
|---|---|---|---|---|---|---|
| Other costs | | | | | | x |

Could you provide an indication of costs, if possible, in FTE/EUR?

*[Free Text]*

**Q29: Please rate the cost-effectiveness of the policy options:**

| | The costs would outweigh the benefits | The costs and benefits would be similar | The benefits would outweigh the costs | Don't know/No answer |
|---|---|---|---|---|
| Policy Option 0: Baseline – No policy action | x | | | |
| Policy Option 1: Voluntary measures | x | | | |
| Policy Option 2: Horizontal legislation | | | x | |
| Policy Option 3: Sector Specific legislation | x | | | |
| Policy Option 4: Mixed approach (regulatory + voluntary measures) | x | | | |

Do you have anything to add?

We think that the balance in choices, even if necessary, is multiplied over the policy options, so they could end up with no clear preferences as an outcome.

**Q30: What would be the overall impact of the policy options on the competitiveness of EU's ICT industry?**

| | Significantly negative | Moderately negative | | No change | | Moderately positive | Significantly positive | Don't know/No answer |
|---|---|---|---|---|---|---|---|---|
| Policy Option 0: Baseline – No policy action | | | | | | | | x |
| Policy Option 1: Voluntary measures | | | | | | | | x |
| Policy Option 2: Horizontal legislation | | | | | | | | x |
| Policy Option 3: Sector Specific legislation | | | | | | | | x |
| Policy Option 4: Mixed approach (regulatory + voluntary measures) | | | | | | | | x |

Do you have anything to add?

*[Free Text]*

**Q31: What would be the overall impact of the policy options on the innovation in EU's ICT industry?**

| | Great decrease | Moderate decrease | | No change | | Moderate increase | Great increase | Don't know/No answer |
|---|---|---|---|---|---|---|---|---|
| Policy Option 0: Baseline – No policy action | | | | | | | | x |
| Policy Option 1: Voluntary measures | | | | | | | | x |
| Policy Option 2: Horizontal legislation | | | | | | | | x |
| Policy Option 3: Sector Specific legislation | | | | | | | | x |
| Policy Option 4: Mixed approach (regulatory + voluntary measures) | | | | | | | | x |

Do you have anything to add?

*[Free Text]*

**Q32: What would be the overall impact of the policy options on fairness in competition in the EU's ICT market? *(i.e. creating a level playing field within the EU's ICT market)***

| | Significantly negative | Moderately negative | | No change | | Moderately positive | Significantly positive | Don't know/No answer |
|---|---|---|---|---|---|---|---|---|
| Policy Option 0: Baseline – No policy action | x | | | | | | | |
| Policy Option 1: Voluntary measures | x | | | | | | | |
| Policy Option 2: Horizontal legislation | | | | | | | x | |
| Policy Option 3: Sector Specific legislation | x | | | | | | | |
| Policy Option 4: Mixed approach (regulatory + voluntary measures) | x | | | | | | | |

Do you have anything to add?

*[Free Text]*

**Q33: What would be the impact of the policy options on the availability of reliable and secure ICT products in the Internal Market?**

| | Significantly negative | Moderately negative | | No change | | Moderately positive | Significantly positive | Don't know/No answer |
|---|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Policy Option 0: Baseline – No policy action | x | | | | | | | |
| Policy Option 1: Voluntary measures | x | | | | | | | |
| Policy Option 2: Horizontal legislation | | | | | | | x | |
| Policy Option 3: Sector Specific legislation | x | | | | | | | |
| Policy Option 4: Mixed approach (regulatory + voluntary measures) | x | | | | | | | |

Do you have anything to add?

*[Free Text]*

**Q34: What would be the impact of the policy options on the trust in ICT products?**

| | Significantly negative | Moderately negative | | No change | | Moderately positive | Significantly positive | Don't know/No answer |
|---|---|---|---|---|---|---|---|---|
| Policy Option 0: Baseline – No policy action | x | | | | | | | |
| Policy Option 1: Voluntary measures | x | | | | | | | |
| Policy Option 2: Horizontal legislation | | | | | | | x | |
| Policy Option 3: Sector Specific legislation | x | | | | | | | |
| Policy Option 4: Mixed approach (regulatory + voluntary measures) | x | | | | | | | |

Do you have anything to add?

*[Free Text]*

**Q35: Do you think that policy option 1 (voluntary measures) potentially would not be coherent with other EU initiatives in the areas of product safety and cybersecurity? (such as the General Product Safety Directive, Product Liability Directive, Radio Equipment Directive, Cybersecurity Act, GDPR, Machinery Directive, Medical Device Regulation, or any other). If yes, please mention potential coherence issues.**

*We do not support policy option 1 as not effective in ensuring consumer protection.*

**Q36: Do you think that policy option 2 (Horizontal legislation) potentially would not be coherent with other EU initiatives in the areas of product safety and cybersecurity? (such as the General Product Safety Directive, Product Liability Directive, Radio Equipment Directive, Cybersecurity Act, GDPR, Machinery Directive, Medical Device Regulation, or any other). If yes, please mention potential coherence issues.**

Marginal coherence problems with other EU directives / regulations are expected but easy and timely solvable.

**Q37: Do you think that policy option 3 (Sector specific legislation) potentially would not be coherent with other EU initiatives in the areas of product safety and cybersecurity? (such as the General Product Safety Directive, Product Liability Directive, Radio Equipment Directive, Cybersecurity Act, GDPR, Machinery Directive, Medical Device Regulation, or any other). If yes, please mention potential coherence issues.**

Marginal coherence problems with other EU directives / regulations are expected but easy and timely solvable.

**Q38: Do you think that policy option 4 (Mixed approach) potentially would not be coherent with other EU initiatives in the areas of product safety and cybersecurity? (such as the General Product Safety Directive, Product Liability Directive, Radio Equipment Directive, Cybersecurity Act, GDPR, Machinery Directive, Medical Device Regulation, or any other). If yes, please mention potential coherence issues.**

*We do not support policy option 4 as not effective in ensuring consumer protection.*

**Q39: What would be the impact of the policy options on fundamental rights (e.g. protection of personal data, consumer protection, protection of liberty and security)?**

| | Significantly negative | Moderately negative | No change | Moderately positive | Significantly positive | Don't know/No answer |
|---|---|---|---|---|---|---|
| Policy Option 0: Baseline – No policy action | x | | | | | |
| Policy Option 1: Voluntary measures | x | | | | | |
| Policy Option 2: Horizontal legislation | | | | | x | |
| Policy Option 3: Sector Specific legislation | x | | | | | |
| Policy Option 4: Mixed approach (regulatory + voluntary measures) | x | | | | | |

Do you have anything to add?

*[Free Text]*

**Q40: To what extent do you agree that the policy options add EU value compared to Member States acting separately?**

| | 1. Strongly Disagree | 2. Somewhat Disagree | 3. Neither agree nor disagree | 4. Somewhat Agree | 5. Strongly Agree | Do not know / No opinion |
|---|---|---|---|---|---|---|
| Policy Option 1: Voluntary measures | ○ | ○ | ○ | ○ | ○ | ○X |
| Policy Option 2: Horizontal legislation | ○ | ○ | ○ | ○ | ○X | ○ |
| Policy Option 3: Sector Specific legislation | ○ | ○ | ○ | ○ | ○ | ○X |
| Policy Option 4: Mixed approach (regulatory + voluntary measures) | ○ | ○ | ○ | ○ | ○ | ○X |

[Only if "No"] Please explain your answer:

*[Free Text]*

ANEC-2021-DIGITAL-CYBER-004

20 MAY 2021