EUROPEAN
COMMISSION

Brussels, 15.9.2022
SWD(2022) 282 final

PART 3/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 283 final}

Subsidiarity Grid

Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) and amending Regulation (EU) 2019/1020

1. Can the Union act? What is the legal basis and competence of the Unions' intended action?

1.1 Which article(s) of the Treaty are used to support the legislative proposal or policy initiative?

The legal basis for this proposal is Article 114 of the Treaty of the Functioning of the European Union, which provides for the adoption of measures to ensure the establishing and functioning of the internal market. The purpose of the proposal is to harmonise cybersecurity requirements for products with digital elements in all Member States and to remove obstacles to the free movement of goods.

Article 114 TFEU may be used as a legal basis to prevent the occurrence of these obstacles resulting from diverging national laws and approaches on how to address the legal uncertainties and gaps in the existing legal frameworks.[1] Furthermore, the Court of Justice has recognised that applying heterogeneous technical requirements could be valid grounds to trigger Article 114 TFEU.[2]

The current EU legislative framework applicable to digital products is based on Article 114, and comprises several pieces of legislation, including on specific products and safety-related aspects or general legislation on product liability. However, it covers only certain aspects linked to the cybersecurity of tangible digital products and, as applicable, software embedded in these products. At national level, Member States are starting to take national measures requiring vendors of digital products to enhance their cybersecurity. At the same time, the cybersecurity of digital products has a particularly strong cross-border dimension, as products manufactured in one country are often used by organisations and consumers across the entire internal market. Incidents that initially concern a single entity or Member State often spread within minutes across organisations, sectors and several Member States.

The various acts and initiatives taken so far at EU and national levels only partially address the problems identified and risk creating a legislative patchwork within the internal market, increasing legal uncertainty for both vendors and users of these products and adding unnecessary burden on companies to comply with a number of requirements for similar types of products.

The proposed Regulation would harmonise and streamline the EU regulatory landscape by introducing cybersecurity requirements for products with digital elements and avoid overlapping requirements stemming from different pieces of legislation. This would create greater legal certainty for operators and users across the Union, as well as a better harmonisation of the European single market, creating more viable conditions for operators aiming at entering the EU market.

[1] CJEU Judgment of the Court (Grand Chamber) of 3 December 2019, Czech Republic v European Parliament and Council of the European Union, Case C-482/17, paragraph 35.

[2] CJEU Judgment of the Court (Grand Chamber) of 2 May 2006, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union, Case C-217/04, paragraphs 62-63.

1.2 Is the Union competence represented by this Treaty article exclusive, shared or supporting in nature?

Shared competence

*Subsidiarity does not apply for policy areas where the Union has **exclusive** competence as defined in Article 3 TFEU[3]. It is the specific legal basis which determines whether the proposal falls under the subsidiarity control mechanism. Article 4 TFEU[4] sets out the areas where competence is shared between the Union and the Member States. Article 6 TFEU[5] sets out the areas for which the Unions has competence only to support the actions of the Member States.*

2. Subsidiarity Principle: Why should the EU act?

2.1 Does the proposal fulfil the procedural requirements of Protocol No. 2[6]:

- Has there been a wide consultation before proposing the act?
- Is there a detailed statement with qualitative and, where possible, quantitative indicators allowing an appraisal of whether the action can best be achieved at Union level?

The Commission carried out an extensive consultation in preparation of the Impact Assessment report. It benefited from consultation activities already carried out in 2021 for the exploratory study contracted by the Commission and implemented by a consortium made of Wavestone, CEPS and ICF to assess the need for horizontal cybersecurity requirements for digital products. To ensure a high level of coherence and comparability of analysis for all potential policy approaches, a second study led by the same consortium was contracted to collect evidence and conduct analyses in the first half of 2022.

In addition to the Commission open public consultation and feedback on the Call for Evidence, the external contractors collected evidence from a variety of stakeholders through targeted interviews with experts covering different domains, focus groups, two workshops and a targeted online consultation. Moreover, to further support evidence based analysis, the Commission has conducted extensive desk research, covering a wide spectrum of policy studies and reports. They have been quoted in the main body of the Impact Assessment.

Both the explanatory memorandum (section 2) and the impact assessment (chapter 3) contain respectively sections on the principles of subsidiarity, for more details see question 2.2. below.

2.2 Does the explanatory memorandum (and any impact assessment) accompanying the Commission's proposal contain an adequate justification regarding the conformity with the principle of subsidiarity?

The strong cross-border nature of cybersecurity in general and the growing number of risks and

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12008E003&from=EN
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12008E004&from=EN
[5] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12008E006:EN:HTML
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016E/PRO/02&from=EN

incidents, which have spill-over effects across borders, sectors and products, mean that the objectives of the present intervention cannot effectively be achieved by Member States alone. National approaches in addressing the problems, and in particular approaches introducing mandatory requirements, will create additional legal uncertainty and legal barriers. Companies could be prevented from seamlessly expanding into other Member States, depriving users of the benefits of their products.

Joint action at EU level is therefore necessary to establish a high level of trust among users, increasing the attractiveness of EU products with digital elements. It would also benefit the digital single market and internal market in general by providing legal certainty and achieving a level playing field for manufacturers of products with digital elements.

Ultimately, the Council Conclusions of 23 May 2022 on the development of the European Union's cyber posture[7] call upon the Commission to propose, by the end of 2022, common cybersecurity requirements for connected devices.

2.3 Based on the answers to the questions below, can the objectives of the proposed action be achieved sufficiently by the Member States acting alone (necessity for EU action)?

The strong cross-border nature of cybersecurity in general and the growing number of risks and incidents, which have spill-over effects across borders, sectors and products, mean that the objectives of the present intervention cannot effectively be achieved by Member States alone. National approaches in addressing the problems, and in particular approaches introducing mandatory requirements, will only create additional legal uncertainty and legal barriers. Companies could be prevented from seamlessly expanding into other Member States, depriving users of the benefits of their products.

Joint action at EU level is therefore necessary to establish a high level of trust among users, increasing the attractiveness of EU products with digital elements. It would also benefit the digital single market and internal market in general by providing legal certainty and achieving a level playing field for manufacturers of products with digital elements.

Ultimately, the Council Conclusions of 23 May 2022 on the development of the European Union's cyber posture[8] call upon the Commission to propose, by the end of 2022, common cybersecurity requirements for connected devices.

(a) Are there significant/appreciable transnational/cross-border aspects to the problems being tackled? Have these been quantified?

The strong cross-border nature of cybersecurity in general and the growing risks and incidents, which have spill-over effects across borders, sectors and products, mean that the objectives of the present intervention cannot effectively be achieved by Member States alone. Taking into account the global nature of digital product markets, Member States face the same risks with respect to the same digital product on their territory. For example, a recent study on infected IoT products across the internal market has revealed that it is the same nine manufacturers in each country that are responsible for placing the highest number of IoT devices on the market that have been infected as a result of vulnerabilities, concluding that "international collaboration among regulators in various countries is a feasible path. This would not only bundle scarce resources on the side of governments, but is also

7 Council conclusions on the development of the European Union's cyber posture (2022)
8 Council conclusions on the development of the European Union's cyber posture (2022)

more likely to influence manufacturer behaviour through collective action. An obvious starting point would be coordination at the level of the European Union."[9]

(b) Would national action or the absence of the EU level action conflict with core objectives of the Treaty[10] or significantly damage the interests of other Member States?

An emerging patchy framework of potentially diverging national rules also risks hampering an open and competitive single market for digital products. Some Member States, such as Germany and Finland have already taken first (non-binding) measures to improve the security of digital products. National approaches in addressing the problems, and in particular approaches introducing mandatory requirements, will only create additional legal uncertainty and legal barriers. Companies could be prevented from seamlessly expanding into other Member States, depriving users of the benefits of their products.

(c) To what extent do Member States have the ability or possibility to enact appropriate measures?

Given the lack of negotiation power of individual users on a global products market with large multinational manufacturers (see *section 2.2.5*), regulation at national level would not be effective. In a 2021 report, the Dutch Safety Board concluded that the digital products market "can hardly be influenced by users in the Netherlands alone. Influencing such a global market requires a larger power block, for example at EU or UN level, or based on joint actions by end users."

(d) How does the problem and its causes (e.g. negative externalities, spill-over effects) vary across the national, regional and local levels of the EU?

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of EUR 5.5 trillion by 2021. Such products suffer from two major problems adding costs for users and the society: (1) a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and (2) an insufficient understanding and access to information by users, preventing them from choosing products with proper cybersecurity features or using them in a secure manner.

The cybersecurity of products with digital elements has a strong cross-border dimension, as products manufactured in one country are often used across the internal market. In addition, incidents initially affecting a single entity or a single Member State often spread within minutes across the entire internal market.

(e) Is the problem widespread across the EU or limited to a few Member States?

The identified problems cumulatively affects the Union as a whole.

[9] Rodríguez et al (2021): "Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections", *20th Annual Workshop on the Economics of Information Security (WEIS 2021)*, for a more detailed discussion of IoT consumer device security,
p. 8

[10] https://europa.eu/european-union/about-eu/eu-in-brief_en

(f) Are Member States overstretched in achieving the objectives of the planned measure?
Member States have very different levels of capabilities to address the current cybersecurity challenges, some being more mature and better resourced than others. Also, the adoption of different and potentially contradictory rules for product, which are mostly sold across the whole EU, would risk creating a very fragmented regulatory landscape.
(g) How do the views/preferred courses of action of national, regional and local authorities differ across the EU?
In order to ensure legal certainty and avoid any further fragmentation of product-related requirements on cybersecurity on the internal market, the open public consultation and the targeted consultation have shown a wide overall **support of various stakeholders**, both industry and national authorities for a horizontal intervention setting out cybersecurity requirements for digital products.
2.4 Based on the answer to the questions below, can the objectives of the proposed action be better achieved at Union level by reason of scale or effects of that action (EU added value)?
(a) Are there clear benefits from EU level action?
Yes, EU level action could lead to a higher level of cybersecurity for all digital products across the Union, legal certainty for economic operators and more informed decision making for use by the customers of products with digital elements.
(b) Are there economies of scale? Can the objectives be met more efficiently at EU level (larger benefits per unit cost)? Will the functioning of the internal market be improved?
The objectives of the initiative can be better achieved at Union level so as to avoid a further fragmentation of the single market into potentially contradictory national frameworks. A single framework regarding cybersecurity requirements for products with digital elements would provide legal certainty and avoid overlapping or contradictory requirements stemming from different pieces of legislation. Harmonised EU requirements would facilitate compliance for vendors of products with digital elements and create more viable conditions for operators aiming at entering the EU market.
(c) What are the benefits in replacing different national policies and rules with a more homogenous policy approach?
Users' trust that products with digital elements acquired in any Member State comply with a harmonised set of requirements would increase their trust in and demand for these products. Given the global and cross-border nature of the digital market and the internet, the intervention would reduce negative cross-border spill-overs and costs to society linked to mitigating risks of non-secure products.

(d) Do the benefits of EU-level action outweigh the loss of competence of the Member States and the local and regional authorities (beyond the costs and benefits of acting at national, regional and local levels)?

The EU initiative would raise the level of cybersecurity for the whole EU by introducing horizontal cybersecurity requirements for products with digital elements. At the same time, the EU initiative will remain for the Member States to carry out the market surveillance and enforcement activities and thus the implementation of the requirements.

(e) Will there be improved legal clarity for those having to implement the legislation?

The proposed Regulation would harmonise the EU regulatory landscape by introducing cybersecurity requirements for products with digital elements and avoid overlapping requirements stemming from different pieces of legislation. This would create greater legal certainty for operators and users across the Union, as well as a better harmonisation of the European single market, creating more viable conditions for operators aiming at entering the EU market.

3. Proportionality: How the EU should act

3.1 Does the explanatory memorandum (and any impact assessment) accompanying the Commission's proposal contain an adequate justification regarding the proportionality of the proposal and a statement allowing appraisal of the compliance of the proposal with the principle of proportionality?

As regards the proportionality of the proposed Regulation, the measures in the policy options considered would not go beyond what is needed to achieve the general and specific objectives and would not impose disproportionate costs. More specifically, the intervention considered would ensure that products with digital elements would be secured throughout their whole life cycle and proportionally to the risks faced through objective-oriented and technology neutral requirements that remain reasonable and generally corresponding to the interest of the entities involved.

The essential cybersecurity requirements in the proposal are building on widely used standards, and the standardisation process that will follow would take into account the technical specificities of the products. This means that where needed for a given risk level, security controls would be adapted. Furthermore, the envisaged horizontal rules would only foresee third-party assessment for critical products. This would only include a narrow share of the market for products with digital elements. The impact on SMEs would depend on their presence in the market of these specific product categories.

Regarding the proportionality of the costs for conformity assessment, notified bodies conducting the third party assessments would take the size of the undertaking into account when setting their fees. A reasonable transition period of 24 months to prepare the implementation would also be provided , giving time to the relevant markets to prepare, while providing a clear direction for R&D investments. Any compliance costs for businesses would be outweighed by the benefits brought by a higher level of security of products with digital elements and ultimately an increase of trust of users in these products.

3.2 Based on the answers to the questions below and information available from any impact assessment, the explanatory memorandum or other sources, is the proposed action an appropriate way to achieve the intended objectives?

Yes, as mentioned in the Impact Assessment and the Explanatory Memorandum, the preferred option would ensure the setting out of specific horizontal cybersecurity requirements for all products with digital elements being placed or made available in the internal market, and would be the only option covering the entire digital supply chain. Non-embedded software, often exposed to vulnerabilities, would also be covered by such regulatory intervention, thus ensuring a coherent approach towards all products with digital elements, with a clear share of responsibilities of various economic operators.

This policy option also brings added value by covering duty of care and whole life cycle aspects after the placement of the products with digital elements on the market, to ensure, among others, appropriate information on security support and provision of security updates. This policy option would also come to most effectively complement the recent review of the NIS framework, by ensuring the prerequisites for a strengthened supply chain security. The preferred option would bring significant benefits to the various stakeholders.

(a) Is the initiative limited to those aspects that Member States cannot achieve satisfactorily on their own, and where the Union can do better?

The requirements in the EU initiative would not go beyond what is needed to achieve the general and specific objectives and would not impose disproportionate costs. Member States have very different levels of capabilities to address the current cybersecurity challenges, some being more mature and better resourced and technically prepared than others, risking to create a very fragmented regulatory landscape, given the strong cross border nature of the problems the initiative aims to tackle.

(b) Is the form of Union action (choice of instrument) justified, as simple as possible, and coherent with the satisfactory achievement of, and ensuring compliance with the objectives pursued (e.g. choice between regulation, (framework) directive, recommendation, or alternative regulatory methods such as co-legislation, etc.)?

A regulatory intervention would entail the adoption of a regulation and not a directive. This is because, for this particular type of product legislation, a regulation would more effectively address the problems identified and meet the objectives formulated, since it is an intervention that is conditioning the placing on the internal market of a very wide category of products. The transposition process in the case of a directive for such intervention could leave too much room for discretion at national level, potentially leading to lack of uniformity of certain essential cybersecurity requirements, legal uncertainty, further fragmentation or even discriminatory situations cross-border, even more taking account of the fact that the products covered could be of multiple purpose or use and that manufacturers can produce multiple categories of such products.

(c) Does the Union action leave as much scope for national decision as possible while achieving satisfactorily the objectives set? (e.g. is it possible to limit the European action to minimum

standards or use a less stringent policy instrument og approach?)
The proposal sets out requirements for national authorities responsible for conformity assessment bodies (notified bodies). It leaves the ultimate responsibility for designating and monitoring notified bodies with the Member State. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies. In accordance with Regulation (EU) 2019/1020, national market surveillance authorities will carry out market surveillance in the territory of that Member State. Member States may choose to designate any existing or new authority to act as market surveillance authority. Moreover, the proposal establishes maximum levels for administrative fines that should be provided in national laws for non-compliance with the obligations laid down in this Regulation.
(d) Does the initiative create financial or administrative cost for the Union, national governments, regional or local authorities, economic operators or citizens? Are these costs commensurate with the objective to be achieved?
According to the Impact Assessment, the preferred option (which has been chosen for the present EU initiative) would add compliance and enforcement costs for businesses, notified bodies and public authorities, including accreditation and market surveillance authorities. For software developers and hardware manufacturers, it will increase the direct compliance costs for new security requirements, documentation and reporting obligations, leading to aggregated costs amounting to up to EUR 29 billion. End users, including business end users, consumers and citizens may face higher prices of digital products. However, they should be seen against the background of the significant benefits as described above.
(e) While respecting the Union law, have special circumstances applying in individual Member States been taken into account?
The proposal sets out requirements for national authorities responsible for conformity assessment bodies (notified bodies). It leaves the ultimate responsibility for designating and monitoring notified bodies with the Member State. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies. Member States will also designate the competent market surveillance authority to carry out supervision and enforcement on the territory of each Member State. Moreover, the proposal establishes maximum levels for administrative fines that should be provided in national laws for non-compliance.