2022.3.28

EU サイバーレジリエンス法のパブコメについて

現在、EU が法令整備中の「サイバーレジリエンス法」についてパブコメを受け付けております。（パブコメ締め切り：5 月 25 日）
「サイバーレジリエンス法」は、EU 市場のデジタル製品及び関連サービスに対する共通のサイバーセキュリティ・ルールを確立することを目的として、EU の NIS 指令やサイバーセキュリティ法などの既存の法令や将来取り得るより高いレベルでの対策を補完するために導入される予定です。
今回のパブコメの結果を踏まえて法案のフレームワークを検討することとなりますので、対象製品・サービスの範囲や、認証の仕組み（自己認証/第三者認証）などは現時点で未定ですが、本パブコメの募集が開始されていることを前広に会員企業へ周知していただけますと幸いです。

○EU のサイト：サイバーレジリエンス法のパブコメの募集
https://digital-strategy.ec.europa.eu/en/news/commission-invites-citizens-and-organisations-share-their-views-european-cyber-resilience-act

○入力方法
以下ページの「Go to consultation>」と書かれた黄色いボタンをクリック。
→「Respond to the questionnaire>」をクリック。ログインして回答。
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

なお、パブコメの入力に当たりましては、質問内容を抜粋した次ページ以降の仮訳をご参考にしていただければと思います。

経済産業省　製造産業局

EU サイバーレジリエンス法のパブコメについて

現在、EU が法令整備中のサイバーレジリエンス法（Cyber Resilience Act）がパブリック・コンサルテーションを実施中。

＜パブコメ締め切り＞：2022 年 5 月 25 日

※以下ページの「Go to consultation>」と書かれた黄色いボタンをクリック。→「Respond to the questionnaire>」をクリック。ログインして回答。

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

＜パブコメ質問内容＞

●セクション1：デジタル製品や使用者のためのサイバーセキュリティ

Section 1: Cybersecurity of digital products and the users of digital products

This section contains questions on the state of cybersecurity of digital products marketed in the European Union and users' ability to choose secure products and use them in a secure manner, and the role that vendors can play in securing products and providing cybersecurity related information on their products.

Sub-section 1.a. – The state of cybersecurity of digital products

Q1: In your view, what is the overall level of cybersecurity of digital products marketed within the European Union (on a scale from 1 to 5 with 5 indicating a very high level of cybersecurity)?

EU 域内で販売されているデジタル製品のサイバーセキィリティレベル全体について、5 段階で示して下さい。（1～5で）

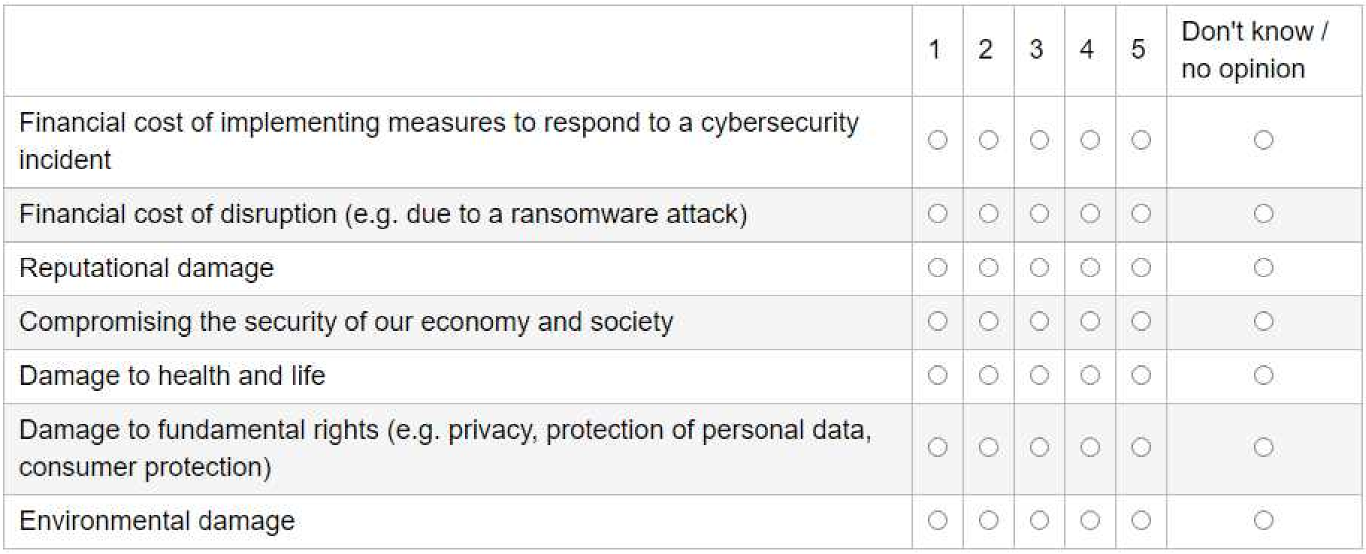
Q2: In your view, during the last five years, how has the level of risk of cybersecurity incidents affecting digital products evolved?

過去5年間に、デジタル製品に影響するサイバーセキュリティインシデントのレベルについて、どのようになったと感じますか。5段階で示して下さい。

Sub-section 1.b. – Consequences of cyber incidents and non-secure digital products

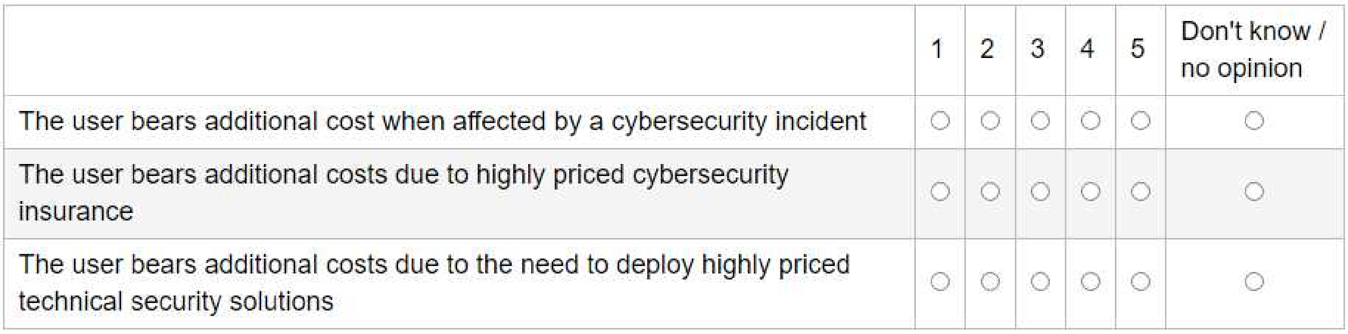
Q3: How would you evaluate the actual impact of cybersecurity incidents affecting digital products on you or your organisation (on a scale from 1 to 5 with 5 indicating a very high negative impact)?

あなた自身やあなたの組織のデジタル製品に影響を与えるサイバーインシデントの実際のインパクトを以下の表の中で表して下さい。（1～5の5段階で）



	1	2	3	4	5	Don't know / no opinion
Financial cost of implementing measures to respond to a cybersecurity incident	○	○	○	○	○	○
Financial cost of disruption (e.g. due to a ransomware attack)	○	○	○	○	○	○
Reputational damage	○	○	○	○	○	○
Compromising the security of our economy and society	○	○	○	○	○	○
Damage to health and life	○	○	○	○	○	○
Damage to fundamental rights (e.g. privacy, protection of personal data, consumer protection)	○	○	○	○	○	○
Environmental damage	○	○	○	○	○	○

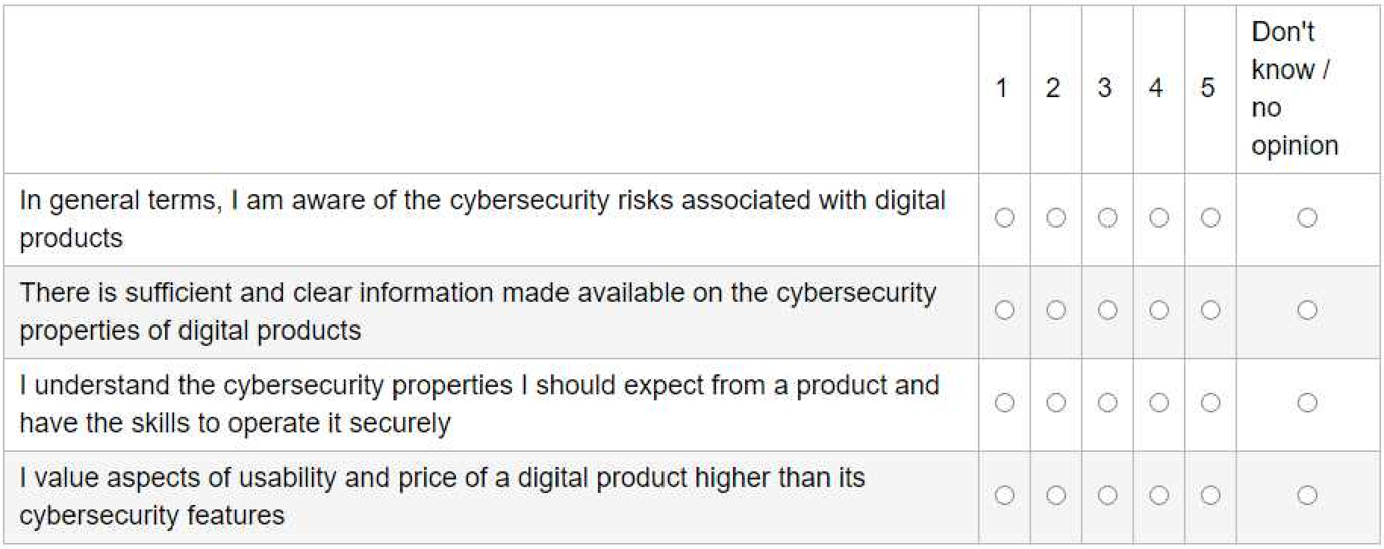
Q4: In your view, if a digital product is not cyber secure, how does it impact the user (on a scale from 1 to 5 with 5 indicating that you fully agree)?
　デジタル製品がセキュアでない場合、ユーザーにとってどのようなインパクトを与えると思いますか。



	1	2	3	4	5	Don't know / no opinion
The user bears additional cost when affected by a cybersecurity incident	○	○	○	○	○	○
The user bears additional costs due to highly priced cybersecurity insurance	○	○	○	○	○	○
The user bears additional costs due to the need to deploy highly priced technical security solutions	○	○	○	○	○	○

Sub-section 1.c. - Trust, cybersecurity awareness and capabilities of users

Q5: To what extent do you agree with the following statements as regards your awareness and understanding of cybersecurity properties of digital products (on a scale from 1 to 5 with 5 indicating that you strongly agree)?
　デジタル製品のサイバーセキュリティ特性についての認識と理解に関して、以下の記載内容にどの程度、賛同しますか。（1～5の 5 段階で）

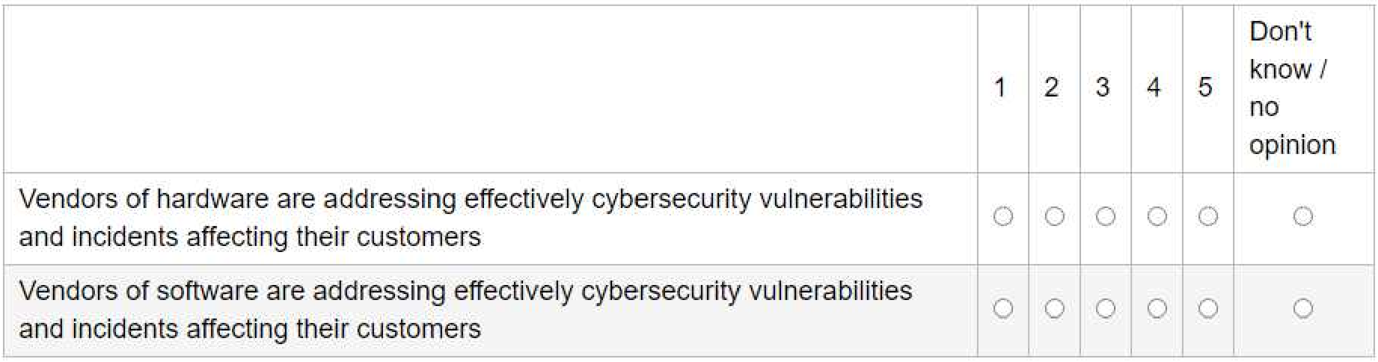


	1	2	3	4	5	Don't know / no opinion
In general terms, I am aware of the cybersecurity risks associated with digital products	○	○	○	○	○	○
There is sufficient and clear information made available on the cybersecurity properties of digital products	○	○	○	○	○	○
I understand the cybersecurity properties I should expect from a product and have the skills to operate it securely	○	○	○	○	○	○
I value aspects of usability and price of a digital product higher than its cybersecurity features	○	○	○	○	○	○

Sub-section 1.d – The role of vendors in providing secure digital products

Q6: To what extent do you agree with the following statements on the role of the vendors? Please rate the following statements on a scale from 1 to 5 (with 5 indicating that you strongly agree).

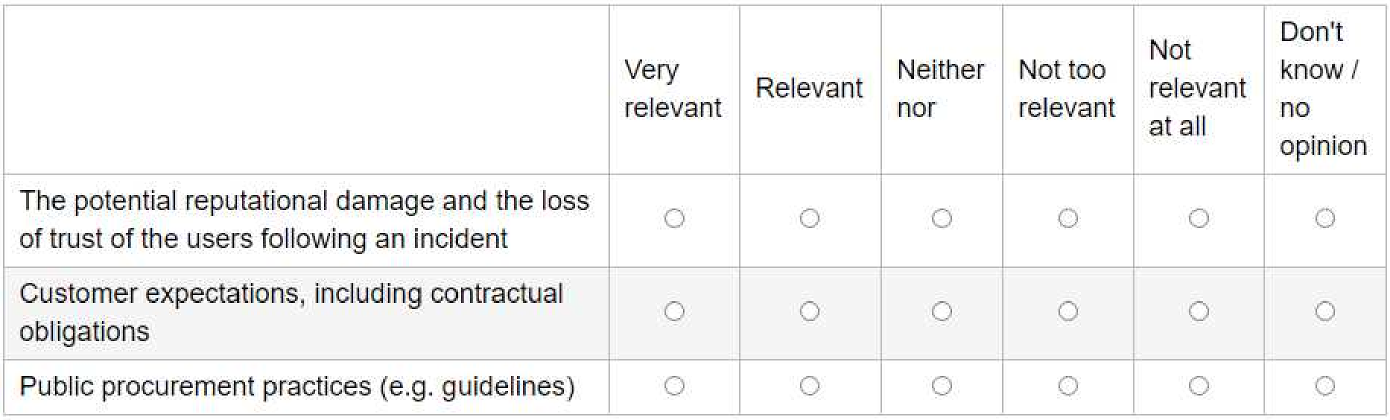
ベンダーの役割に関する以下の記載について、どの程度、賛同しますか。（１～5の5段階で）



	1	2	3	4	5	Don't know / no opinion
Vendors of hardware are addressing effectively cybersecurity vulnerabilities and incidents affecting their customers	○	○	○	○	○	○
Vendors of software are addressing effectively cybersecurity vulnerabilities and incidents affecting their customers	○	○	○	○	○	○

Q7: If you are a vendor: which of the following aspects have the biggest impact on your decision related to cybersecurity of your digital product?

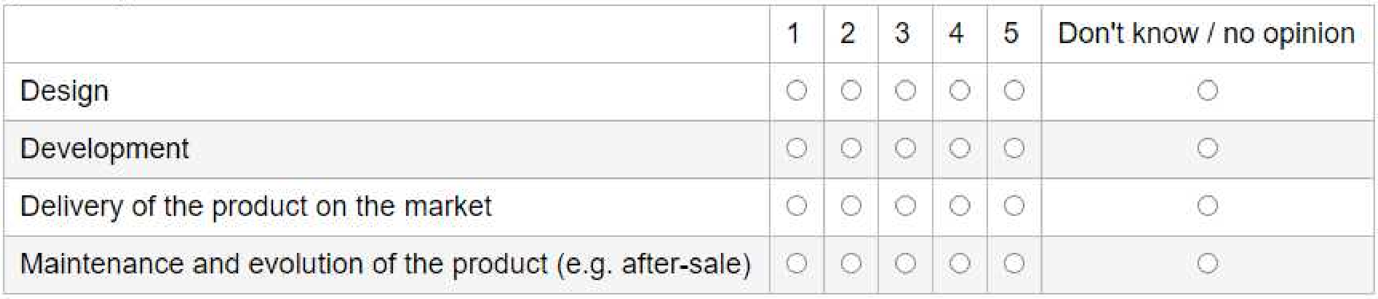
もし、あなたがベンダーの場合、あなたのデジタル製品におけるサイバーセキュリティに関する意見に最も影響を与える要因は以下のうちどれですか？



	Very relevant	Relevant	Neither nor	Not too relevant	Not relevant at all	Don't know / no opinion
The potential reputational damage and the loss of trust of the users following an incident	○	○	○	○	○	○
Customer expectations, including contractual obligations	○	○	○	○	○	○
Public procurement practices (e.g. guidelines)	○	○	○	○	○	○

Q8: To what extent are hardware manufacturers and software developers taking the cybersecurity of their digital products into account in each of the following phases of the product lifecycle (on a scale from 1 to 5 with 5 indicating that cybersecurity is taken very seriously)?

ハードウェア製造者やソフトウェア開発者は、製品のライフサイクルにおける以下の各フェーズにおいてどの程度デジタル製品におけるサイバーセキュリティを考慮していますか。(1～5の 5 段階で)



	1	2	3	4	5	Don't know / no opinion
Design	○	○	○	○	○	○
Development	○	○	○	○	○	○
Delivery of the product on the market	○	○	○	○	○	○
Maintenance and evolution of the product (e.g. after-sale)	○	○	○	○	○	○

●セクション2：デジタル製品におけるサイバーセキュリティの改善

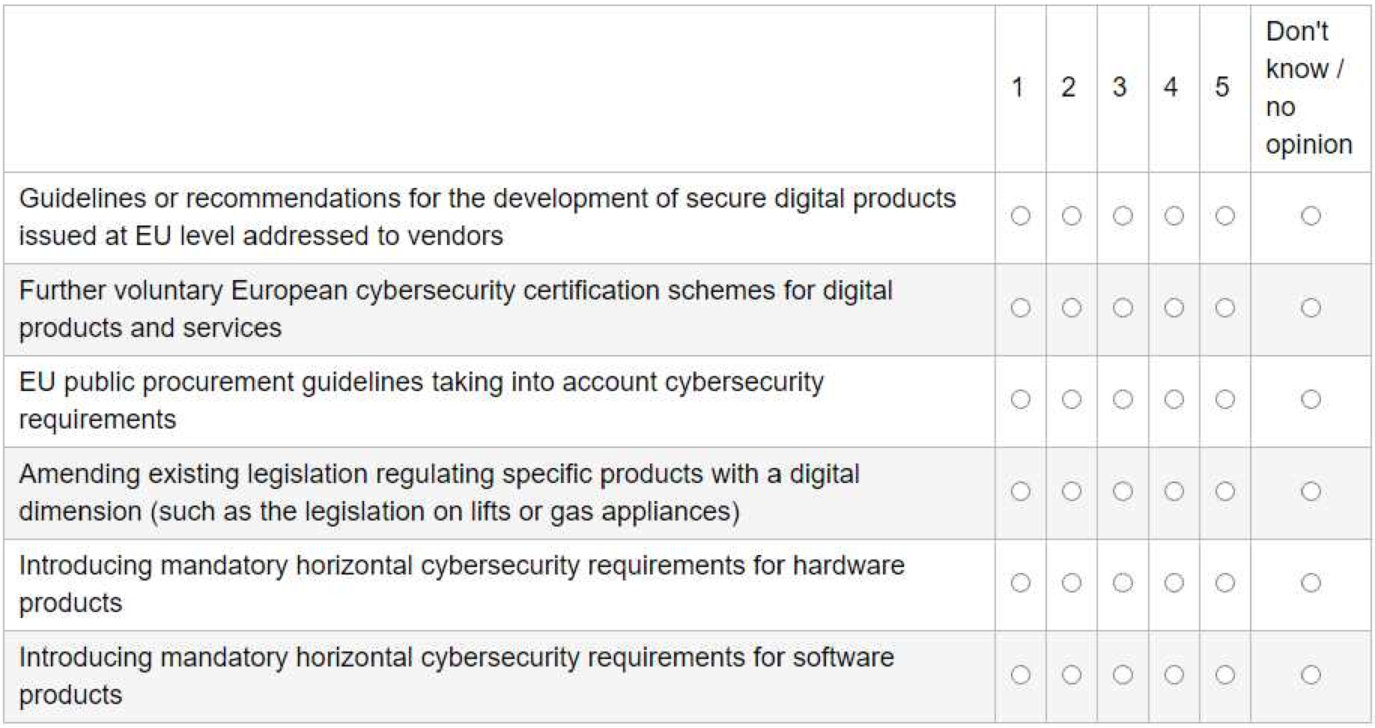
Section 2: Improving the cybersecurity of digital products

This section explores various policy options to improve the cybersecurity of digital products. This includes also questions on the types of products to be covered by an intervention, on other relevant legislation, on security requirements, on risk as well as ways to assess the conformity of manufacturers.

Sub-section 2.a. – Exploring ways to make digital products more secure

Q9: To what extent do you think that the following measures could be effective in raising the level of cybersecurity of digital products marketed in the Union (on a scale from 1 to 5 with 5 indicating that a measure would be very effective)?

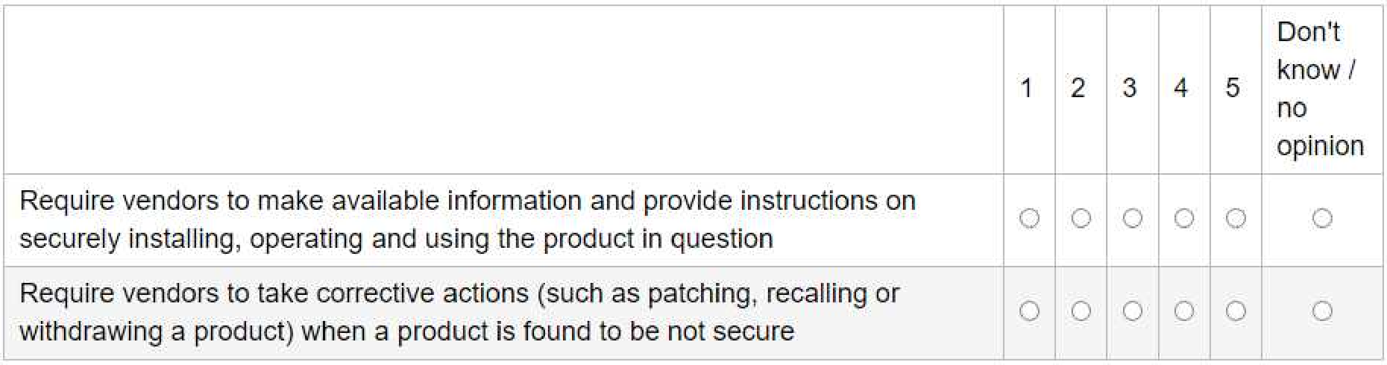
EU 域内で販売されているデジタル製品におけるサイバーセキュリティのレベルを向上させる点で以下の方法がどの程度効果的だと思いますか。(1～5の5段階で)



	1	2	3	4	5	Don't know / no opinion
Guidelines or recommendations for the development of secure digital products issued at EU level addressed to vendors	○	○	○	○	○	○
Further voluntary European cybersecurity certification schemes for digital products and services	○	○	○	○	○	○
EU public procurement guidelines taking into account cybersecurity requirements	○	○	○	○	○	○
Amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances)	○	○	○	○	○	○
Introducing mandatory horizontal cybersecurity requirements for hardware products	○	○	○	○	○	○
Introducing mandatory horizontal cybersecurity requirements for software products	○	○	○	○	○	○

Q10: How would you assess the impact of the following measures on the level of cybersecurity of digital products and of the consumers/organisations using such products (on a scale from 1 to 5 with 5 indicating that a measure would have a very high impact)?

デジタル製品やそれを使用する消費者/組織のサイバーセキュリティレベルに関して、以下の方法をどの程度のインパクトがあると評価しますか。

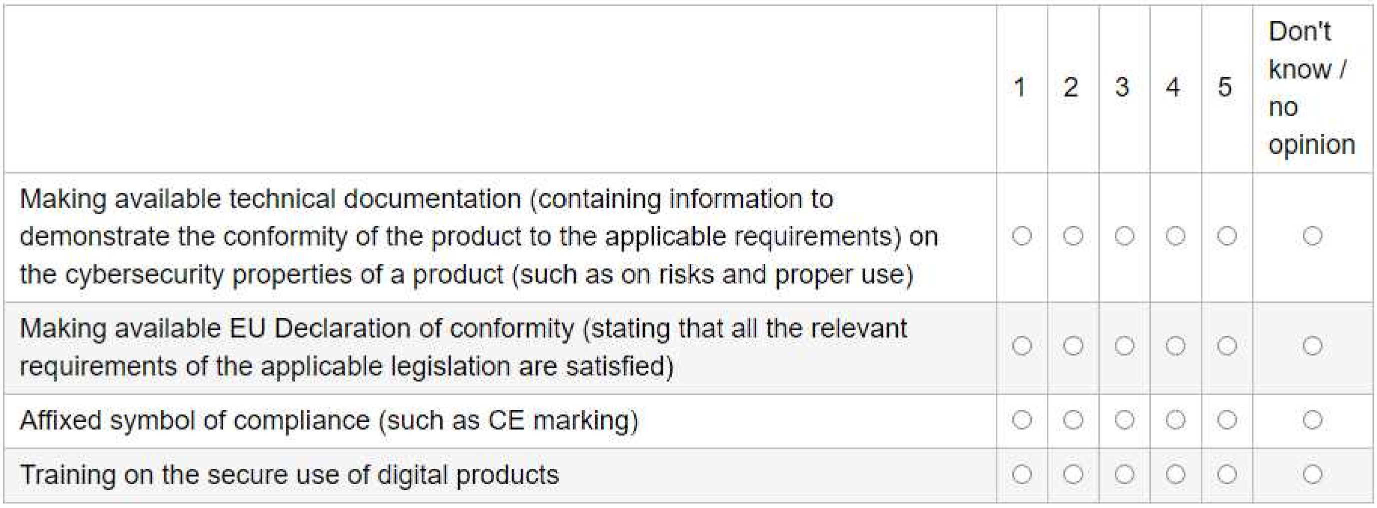


	1	2	3	4	5	Don't know / no opinion
Require vendors to make available information and provide instructions on securely installing, operating and using the product in question	○	○	○	○	○	○
Require vendors to take corrective actions (such as patching, recalling or withdrawing a product) when a product is found to be not secure	○	○	○	○	○	○

Sub-section 2.b. – Exploring ways to make users more aware

Q11: How would you assess the relevance of the following measures for the users' ability to evaluate the cybersecurity properties of a digital product and to make better informed purchase or usage decisions (on a scale from 1 to 5 with 5 indicating that a measure is very relevant)?

デジタル製品のサイバーセキュリティ特性を評価し、十分な情報に基づいて購入又は使用する点におけるユーザーの能力に対し、以下の方法がどの程度関連すると思いますか。（1～5の 5 段階で）

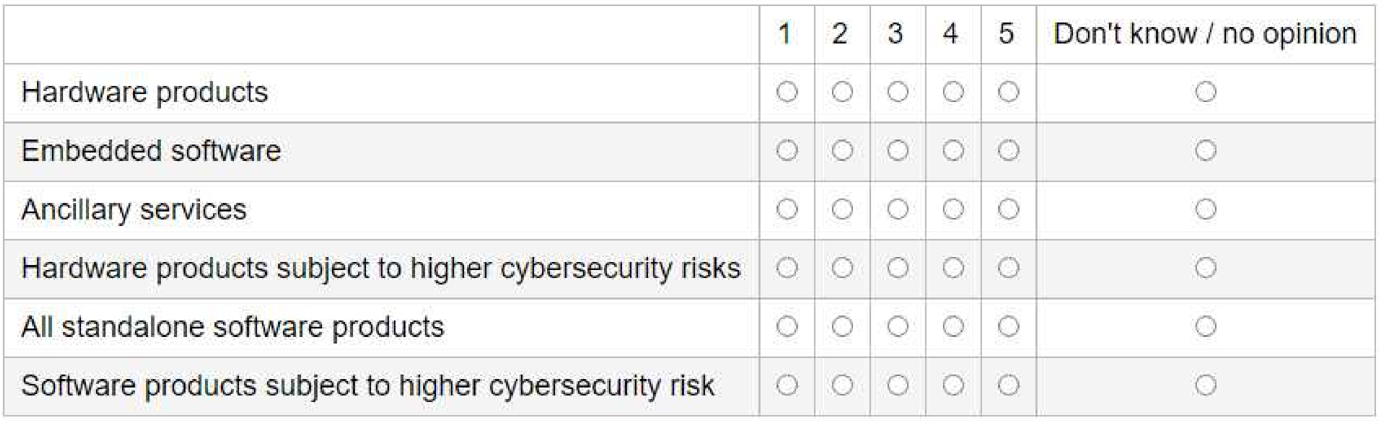


	1	2	3	4	5	Don't know / no opinion
Making available technical documentation (containing information to demonstrate the conformity of the product to the applicable requirements) on the cybersecurity properties of a product (such as on risks and proper use)	○	○	○	○	○	○
Making available EU Declaration of conformity (stating that all the relevant requirements of the applicable legislation are satisfied)	○	○	○	○	○	○
Affixed symbol of compliance (such as CE marking)	○	○	○	○	○	○
Training on the secure use of digital products	○	○	○	○	○	○

Sub-section 2.c. – Digital products to be covered by a European initiative

Q12: To what extent do you agree that subjecting certain products marketed in the Union to cybersecurity requirements would be effective (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

EU 域内で販売されている以下の製品をサイバーセキュリティ要件に遵守させることが効果的であるという点にどの程度賛同しますか。（1～5の 5 段階で）

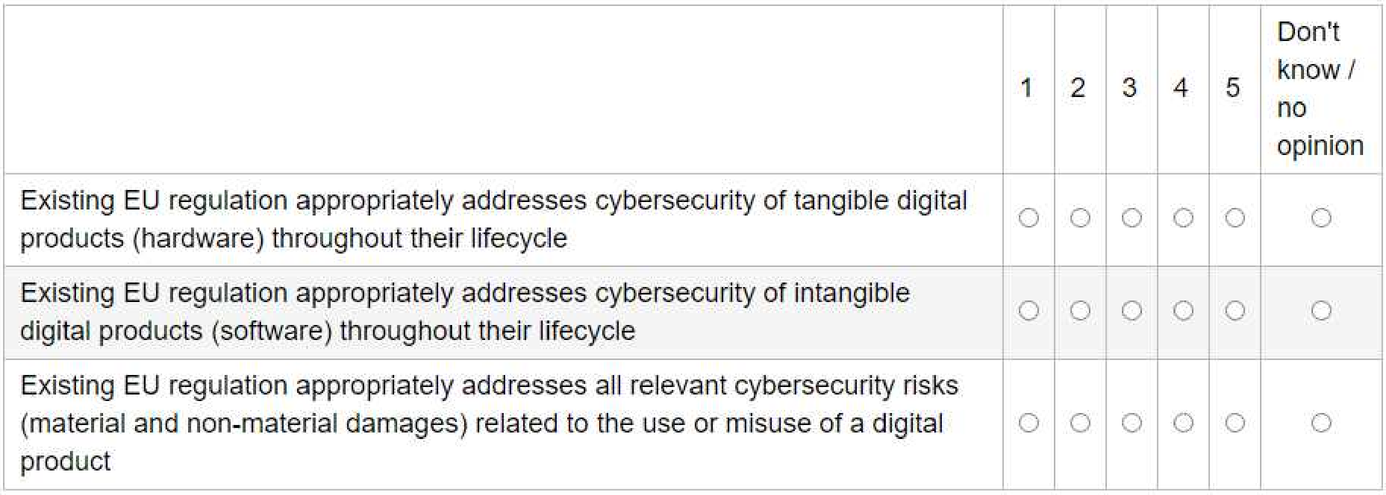


	1	2	3	4	5	Don't know / no opinion
Hardware products	○	○	○	○	○	○
Embedded software	○	○	○	○	○	○
Ancillary services	○	○	○	○	○	○
Hardware products subject to higher cybersecurity risks	○	○	○	○	○	○
All standalone software products	○	○	○	○	○	○
Software products subject to higher cybersecurity risk	○	○	○	○	○	○

Sub-section 2.d. – Existing legislation on the cybersecurity of digital products

Q13: To what extent do you agree with the following statements about how cybersecurity is addressed in existing EU legislation (e.g. the General Product Safety Directive and the Machinery Directive, both currently under review; the Delegated Regulation of 29 October 2021 under the Radio Equipment Directive) (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

既存の EU 法令におけるサイバーセキュリティの扱いについて、以下の記載にどの程度賛同しますか。（例：現在レビュー中の一般製品安全指令、機械指令、及び無線機器指令に基づく 2021 年 10 月 29 日の委任規則）（1～5の 5 段階で）



	1	2	3	4	5	Don't know / no opinion
Existing EU regulation appropriately addresses cybersecurity of tangible digital products (hardware) throughout their lifecycle	○	○	○	○	○	○
Existing EU regulation appropriately addresses cybersecurity of intangible digital products (software) throughout their lifecycle	○	○	○	○	○	○
Existing EU regulation appropriately addresses all relevant cybersecurity risks (material and non-material damages) related to the use or misuse of a digital product	○	○	○	○	○	○

Q14: In the absence of horizontal cybersecurity requirements at European level, Member States could adopt national laws placing certain requirements on vendors. To what extent do you agree that there is a risk of increasing costs and legal uncertainty for market stakeholders, in the absence of an EU initiative? (on a scale from 1 to 5 with 5 indicating you fully agree)?

欧州レベルでの水平的なサイバーセキュリティ要件がない場合、EU 加盟国はベンダーに特定の要件を課す国内法を採用する可能性があります。このような EU のイニシアティブがない場合、市場のステークホルダーにとって、コストの増加や法的不確実性が生じるリスクがあることにどの程度賛同しますか。（1～5の5段階で）

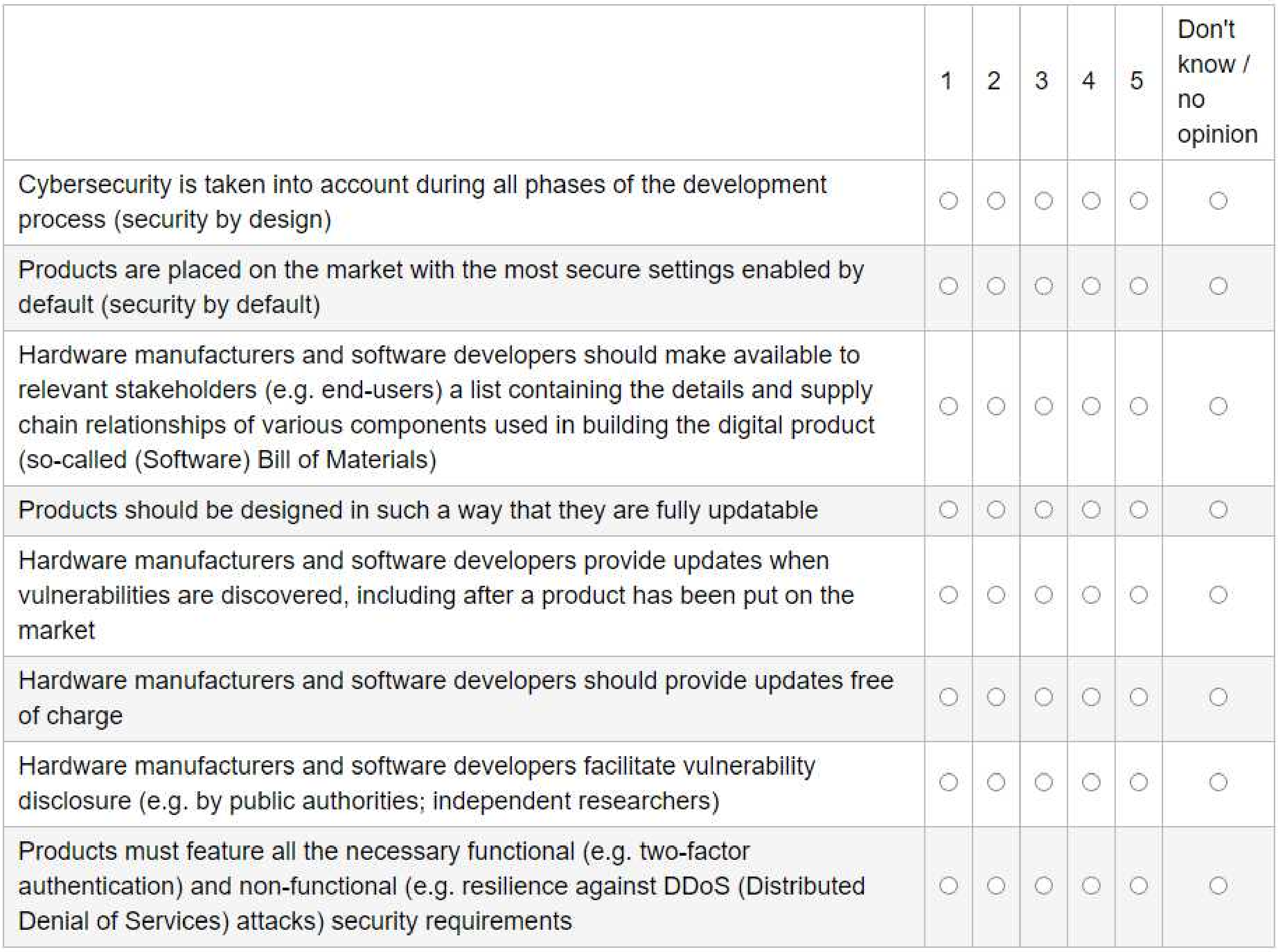
Q15: If you are a vendor: are your digital products subject to legal requirements as regards their cybersecurity? In your answer, please take into account European, national but also legislation stemming from third countries.
もし、あなたがベンダーの場合、あなたのデジタル製品は、EU 法令・国内法・第三国の法令のサイバーセキュリティに関する法的要件を遵守していますか。（Yes/No）

Sub-section 2.e. – Cybersecurity requirements for digital products

Q16: Should hardware manufacturers and software developers be responsible for the full life cycle of a digital product (such as by being required to provide updates)?

ハードウェア製造者やソフトウェア開発者はデジタル製品のライフサイクル全てに責任を負うべきと思いますか？（例えば、更新を提供する必要性など）（Yes/No）

Q17: To what extent can the following approaches contribute to the cybersecurity of a digital product (on a scale from 1 to 5 with 5 indicating that a measure would be very effective)?
デジタル製品におけるサイバーセキュリティのために、以下のアプローチがどの程度貢献すると思いますか。（1～5の5段階で）



	1	2	3	4	5	Don't know / no opinion
Cybersecurity is taken into account during all phases of the development process (security by design)	○	○	○	○	○	○
Products are placed on the market with the most secure settings enabled by default (security by default)	○	○	○	○	○	○
Hardware manufacturers and software developers should make available to relevant stakeholders (e.g. end-users) a list containing the details and supply chain relationships of various components used in building the digital product (so-called (Software) Bill of Materials)	○	○	○	○	○	○
Products should be designed in such a way that they are fully updatable	○	○	○	○	○	○
Hardware manufacturers and software developers provide updates when vulnerabilities are discovered, including after a product has been put on the market	○	○	○	○	○	○
Hardware manufacturers and software developers should provide updates free of charge	○	○	○	○	○	○
Hardware manufacturers and software developers facilitate vulnerability disclosure (e.g. by public authorities; independent researchers)	○	○	○	○	○	○
Products must feature all the necessary functional (e.g. two-factor authentication) and non-functional (e.g. resilience against DDoS (Distributed Denial of Services) attacks) security requirements	○	○	○	○	○	○

Sub-section 2.f. – The role of risk

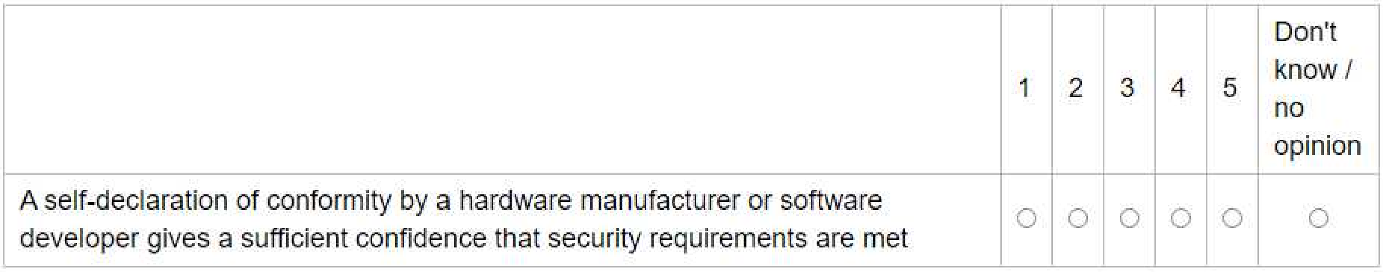
Q18: Under this initiative, hardware manufacturers and software developers would need to demonstrate their compliance with cybersecurity requirements. Should digital products with a higher risk be subject to a stricter process of demonstrating conformity with these requirements?

本イニシアティブでは、ハードウェア製造者とソフトウェア開発者は、サイバーセキュリティ要件への準拠を実証する必要があります。リスクの高いデジタル製品は、これらの要件への適合を実証するためにより厳格なプロセスの対象とすべきと思いますか。（Yes/No）

Sub-section 2.g. – Demonstrating compliance with security requirements

Q19: How would you assess the following statement regarding self-declaration as a way for hardware manufacturers and software developers to demonstrate compliance with security requirements (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

ハードウェア製造者とソフトウェア開発者がセキュリティ要件への準拠を実証する方法として、自己宣言に関する以下の記載をどのように評価しますか。（１～5の 5 段階で）



	1	2	3	4	5	Don't know / no opinion
A self-declaration of conformity by a hardware manufacturer or software developer gives a sufficient confidence that security requirements are met	○	○	○	○	○	○

Q20: If you consider that self-declaration is not enough to demonstrate compliance with security requirements, do you think that the involvement of a third party should be required under certain circumstances?
セキュリティ要件への準拠を実証する方法として、自己宣言が不十分であると考える場合、特定の状況下では第三者機関の関与が必要だと思いますか。（Yes/No）

●セクション3：潜在的な規制措置のステークホルダーへの影響

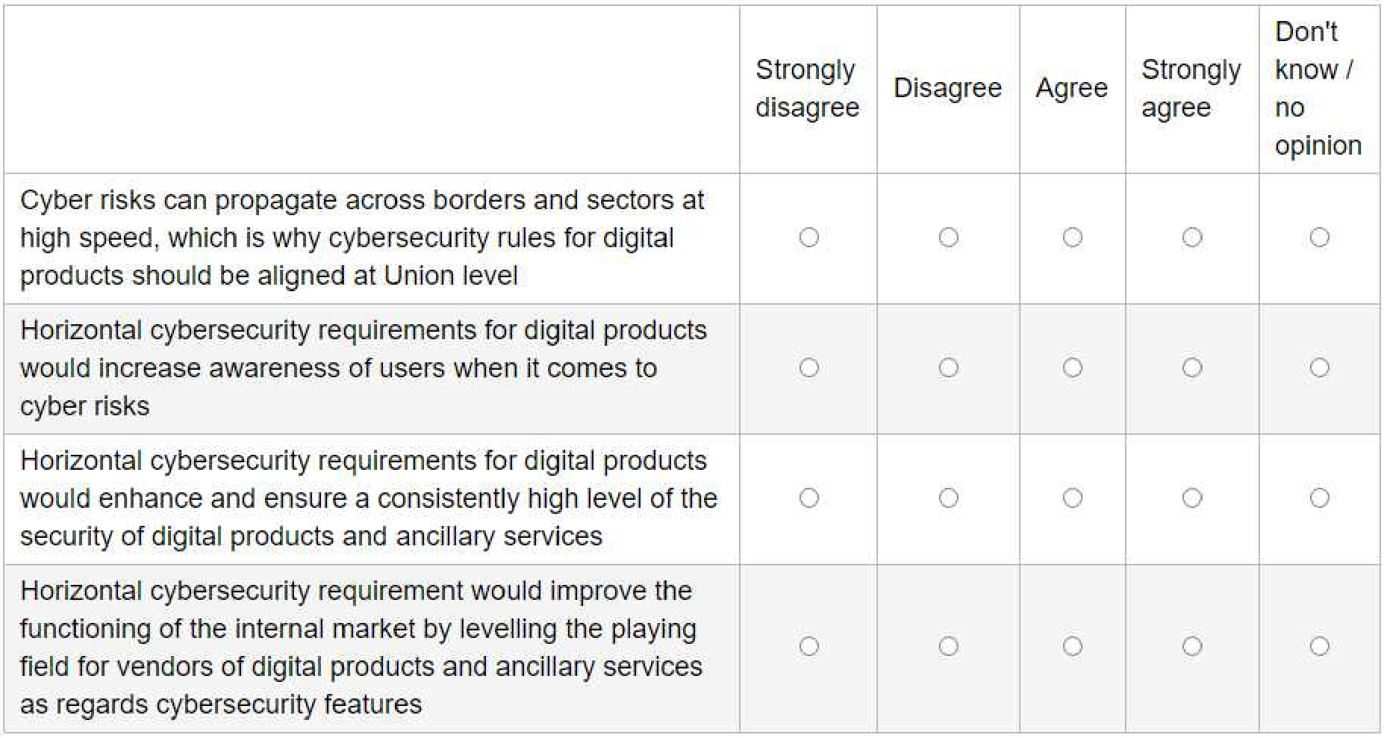
Section 3: Stakeholder impact of potential regulatory measures

This section focuses on the EU added value and estimated impacts of potential measures on stakeholders.

Sub-section 3.a. – Relevance of horizontal requirements for digital products at European level

Q21: To what extent do you agree with the following statements that look into the potential effectiveness of an EU initiative on horizontal (cross-sectoral) cybersecurity requirements?

水平的（分野横断的）なサイバーセキュリティ要件に関する EU のイニシアティブの潜在的な有効性を検討するための以下の記述にどの程度賛同しますか。



	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Cyber risks can propagate across borders and sectors at high speed, which is why cybersecurity rules for digital products should be aligned at Union level	○	○	○	○	○
Horizontal cybersecurity requirements for digital products would increase awareness of users when it comes to cyber risks	○	○	○	○	○
Horizontal cybersecurity requirements for digital products would enhance and ensure a consistently high level of the security of digital products and ancillary services	○	○	○	○	○
Horizontal cybersecurity requirement would improve the functioning of the internal market by levelling the playing field for vendors of digital products and ancillary services as regards cybersecurity features	○	○	○	○	○

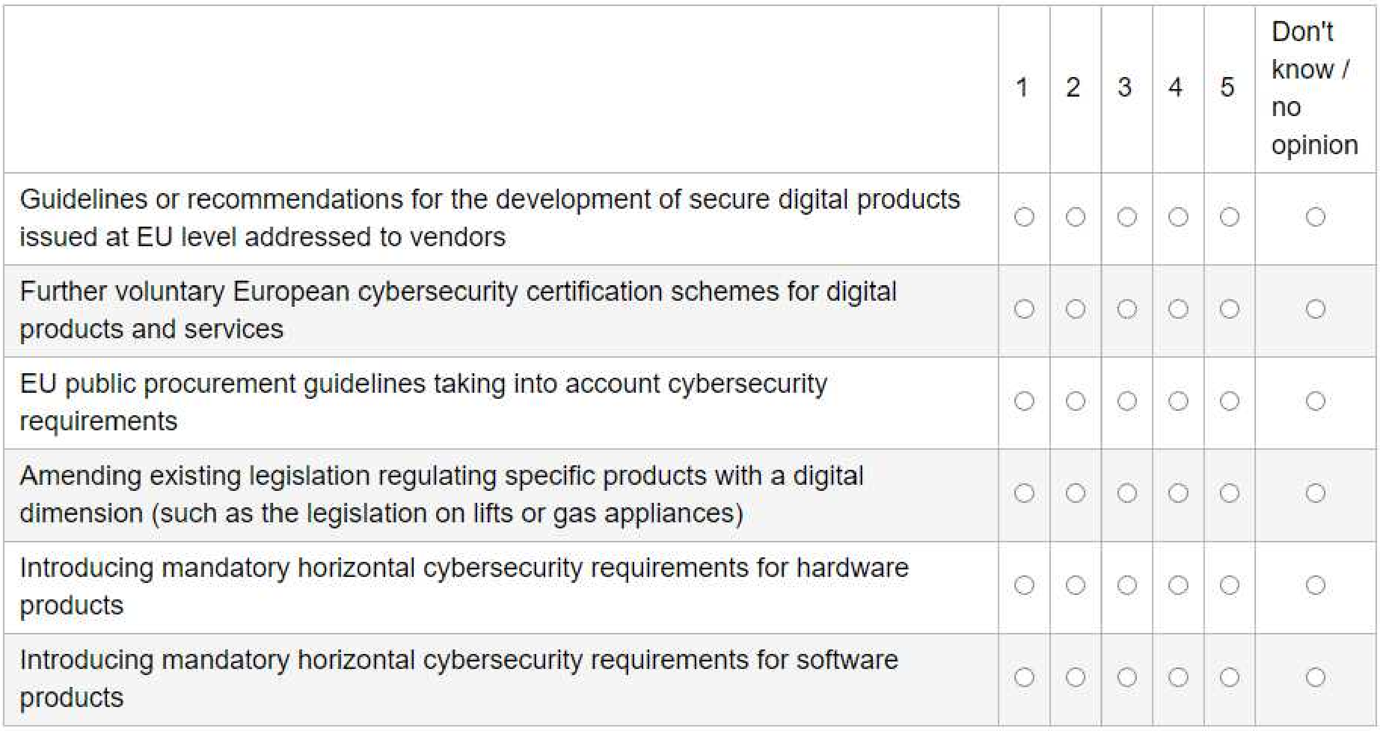
Q22: The EU Action Plan on synergies between civil, defence and space industries underlines the importance of promoting and applying common standards across sectors and the increased relevance of digital products that are used both in a civilian and military context (‘dual-use products’). To what extent could horizontal requirements applying to digital dual-use products contribute to moving the security performance of such products closer to the needs of the defense community and to raising the overall level of cybersecurity in civilian uses (on a scale from 1 to 5 with 5 indicating a very positive contribution)?

民間・防衛・宇宙産業間の相乗効果に関するEU行動計画は、分野横断の共通の基準を推進/適用することの重要性と、民間・軍事の両方の文脈で使用されるデジタル製品（デュアル・ユース製品）の関連性の向上を強調しています。デジタルデュアルユース製品に適用される水平的要件は、そのような製品のセキュリティパフォーマンスを防衛業界のニーズに近づけ、民間用途のサイバーセキュリティの全体的なレベル向上にどの程度貢献できると思いますか。（1～5の5段階で）

Sub-section 3.b. – Impact on your organisation in terms of cost

Q23: How would you assess the impact of the following types of intervention on the costs of your organisation (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly)?

以下のタイプの介入について、組織のコストに与える影響をどのように評価しますか。（1～5の5段階で）

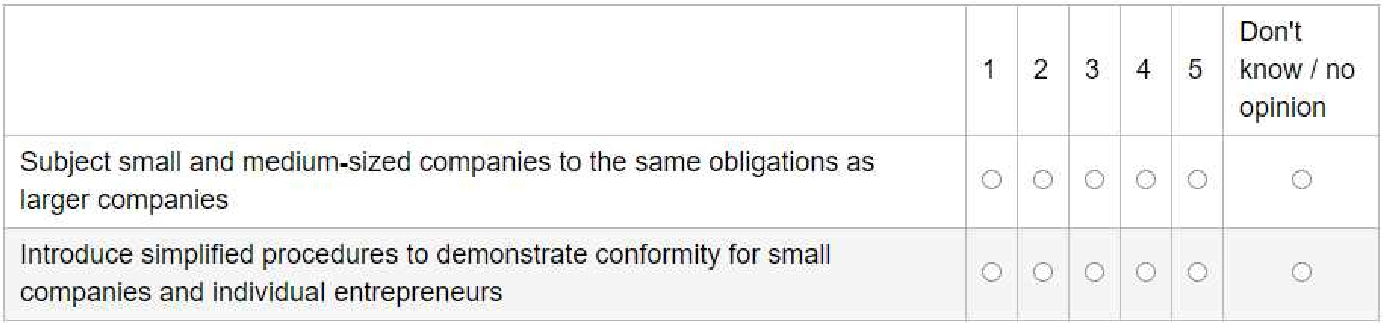


	1	2	3	4	5	Don't know / no opinion
Guidelines or recommendations for the development of secure digital products issued at EU level addressed to vendors	○	○	○	○	○	○
Further voluntary European cybersecurity certification schemes for digital products and services	○	○	○	○	○	○
EU public procurement guidelines taking into account cybersecurity requirements	○	○	○	○	○	○
Amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances)	○	○	○	○	○	○
Introducing mandatory horizontal cybersecurity requirements for hardware products	○	○	○	○	○	○
Introducing mandatory horizontal cybersecurity requirements for software products	○	○	○	○	○	○

Sub-section 3.c. – Regulatory burden and costs for small and medium-sized companies

Q24: Which of the following approaches would in your view ensure that small and medium-sized hardware manufacturers and software developers, including individual entrepreneurs, are subject to proportionate obligations (balance between administrative burden and compliance costs on the one hand and a high level of cybersecurity on the other hand) under a European legislation introducing mandatory horizontal cybersecurity requirements (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

サイバーセキュリティにおける水平的な強制要件を取り入れた EU 法令において、個人起業家を含む中小のハードウェア製造者やソフトウェア開発者がどの程度の義務を負うべきと考えますか。（行政的な負荷やコンプライアンスコストと高レベルでのサイバーセキュリティとをバランスさせる意味で）（１～5の 5 段階で）



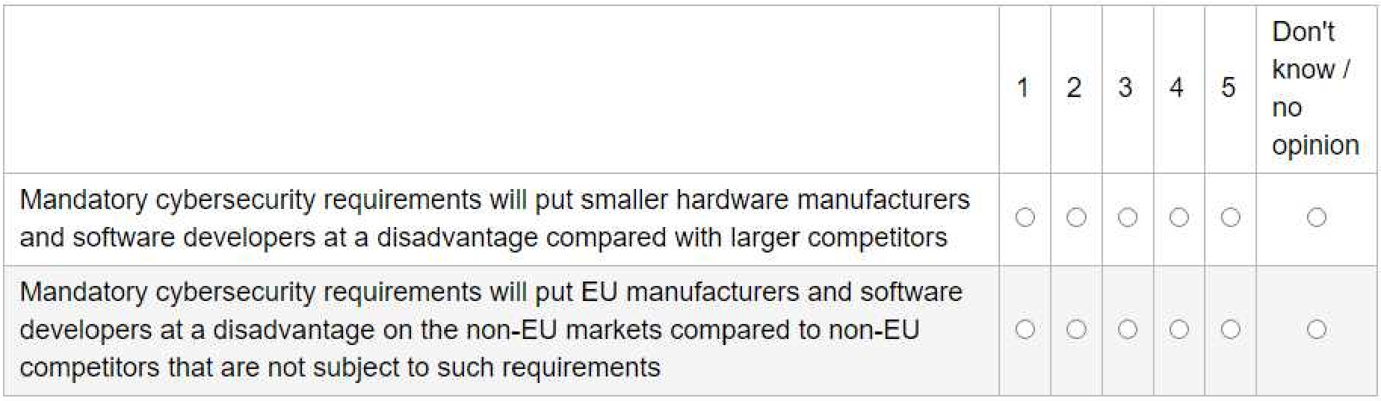
	1	2	3	4	5	Don't know / no opinion
Subject small and medium-sized companies to the same obligations as larger companies	○	○	○	○	○	○
Introduce simplified procedures to demonstrate conformity for small companies and individual entrepreneurs	○	○	○	○	○	○

Sub-section 3.d. – Impact on competition

Q25: An EU initiative laying down mandatory horizontal cybersecurity requirements would apply to all vendors placing products on the internal market, irrespective of their origin and location. To what extent

would you agree with the following statements regarding the impact on competition of such an initiative (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

サイバーセキュリティにおける水平的な強制要件を規定するEUイニシアティブは、製品の原産地や場所に関わらず、製品を国内市場に上市する全てのベンダーに適用されます。そのようなイニシアティブが競争環境にどの程度影響を与えると思いますか。（1～5の5段階で）

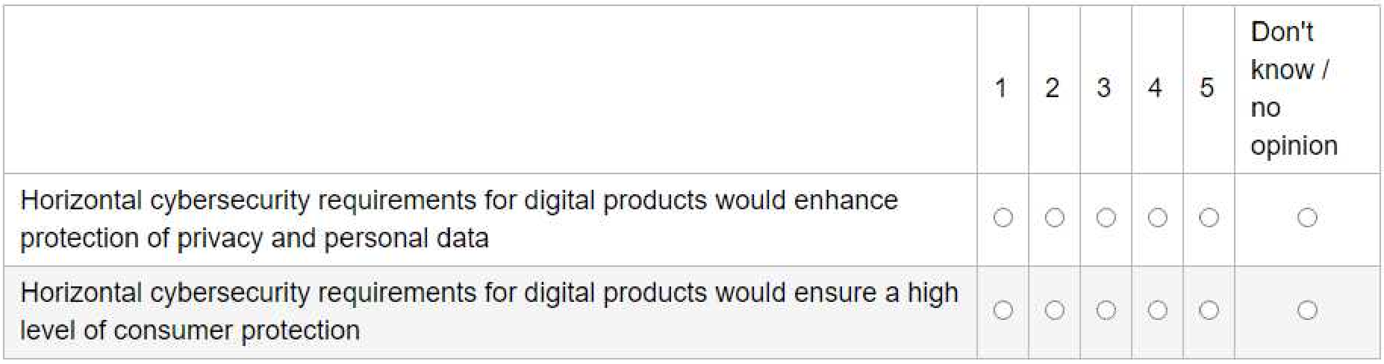


	1	2	3	4	5	Don't know / no opinion
Mandatory cybersecurity requirements will put smaller hardware manufacturers and software developers at a disadvantage compared with larger competitors	○	○	○	○	○	○
Mandatory cybersecurity requirements will put EU manufacturers and software developers at a disadvantage on the non-EU markets compared to non-EU competitors that are not subject to such requirements	○	○	○	○	○	○

Sub-section 3.e. – Impact on fundamental rights

Q26: To what extent to you agree with the following statements regarding the impact of horizontal cybersecurity requirements on fundamental rights (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

基本的権利に関し、水平的なサイバーセキュリティ要件の影響について、次の記載にどの程度賛同しますか。（1～5の5段階で）



	1	2	3	4	5	Don't know / no opinion
Horizontal cybersecurity requirements for digital products would enhance protection of privacy and personal data	○	○	○	○	○	○
Horizontal cybersecurity requirements for digital products would ensure a high level of consumer protection	○	○	○	○	○	○

●セクション4：その他

Section 4: Other issues

This section focuses on cybersecurity challenges for the internal market other than those related to digital products.

Q27: In addition to the issues above, are there other cybersecurity related challenges not directly linked to the cybersecurity of products that you think the Cyber Resilience Act should include to enhance the cyber resilience of the internal market? Please elaborate

上記の内容に加えて、製品のサイバーセキュリティに直接は関係しないもののサイバーレジリエンス法に含めるべき課題はありますか。