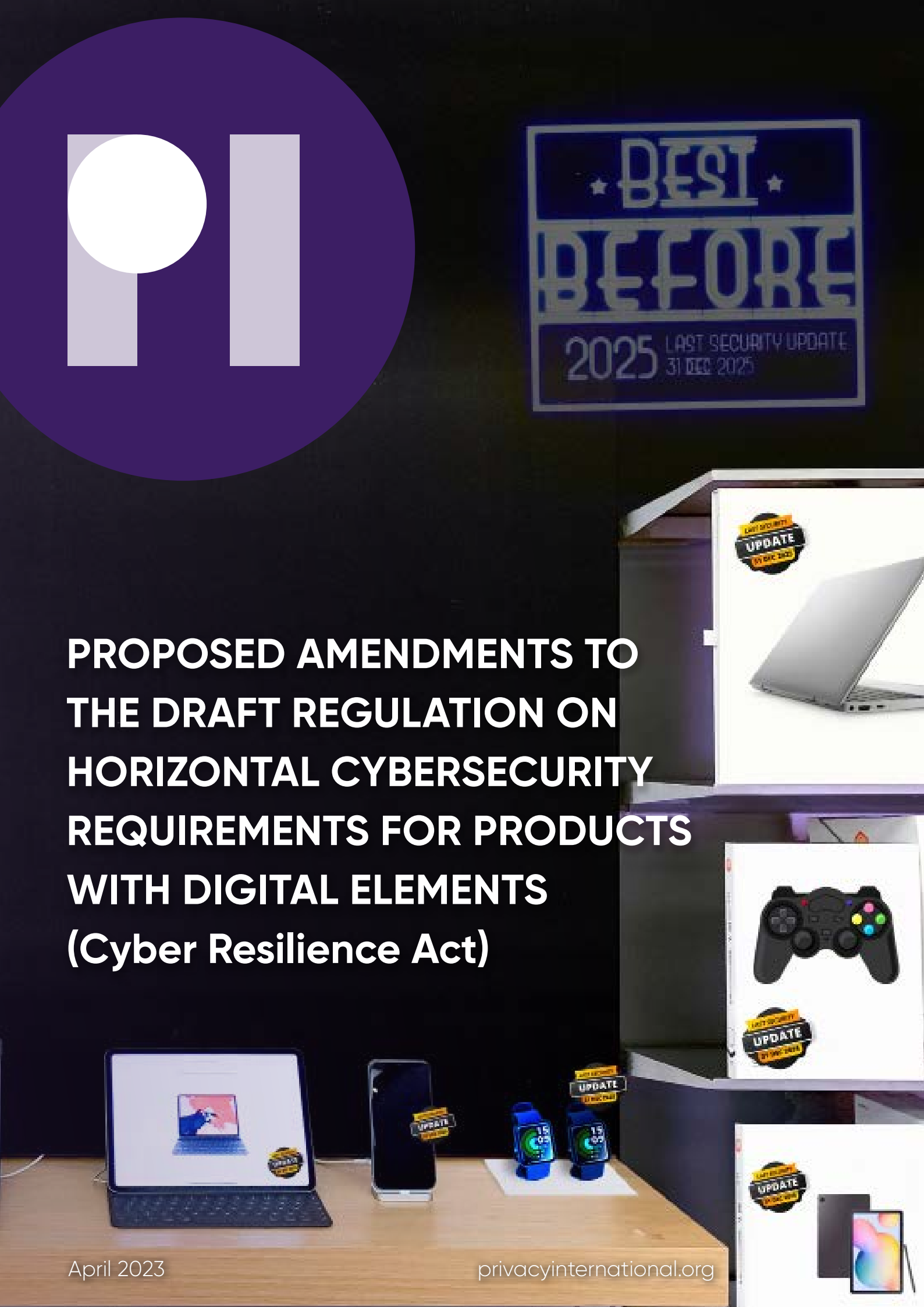


PROPOSED AMENDMENTS TO THE DRAFT REGULATION ON HORIZONTAL CYBERSECURITY REQUIREMENTS FOR PRODUCTS WITH DIGITAL ELEMENTS (Cyber Resilience Act)

April 2023

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.

creative commons

Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission.This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;
- You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright.

For more information please go to www.creativecommons.org.

Photo by Aedrian on Unsplash

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

PROPOSED AMENDMENTS TO THE DRAFT REGULATION ON HORIZONTAL CYBERSECURITY REQUIREMENTS FOR PRODUCTS WITH DIGITAL ELEMENTS (Cyber Resilience Act)

April 2023

INTRODUCTION

Privacy International welcomes the aim of the Cyber Resilience Act to bolster cybersecurity rules to ensure more secure hardware and software products. Nevertheless, we note that the proposal put forward by the European Commission contains certain shortcomings which could both hamper innovation and harm consumers who are increasingly relying on digital products and services.

It is essential these shortcomings, detailed below, are effectively addressed by the EU co-legislators through the introduction of specific amendments to ensure that the aim of the proposed Regulation is not undermined, and that consumers' devices and data remain secure in our connected world. Notwithstanding any other issues that could potentially arise in the context of the Commission's proposal, **the scope of the present brief is limited to business-to-consumer (B2C) concerns with regard to the duration of security software support, the handling of software vulnerabilities, and free and open-source software (FOSS).**

Privacy International (PI) is a global, not-for-profit organization that campaigns against companies and governments who exploit our data and technologies. We do not accept any funding from industry, and we have a strict policy about the circumstances under which we accept grants in order to ensure our independence from state actors and private organizations. Given our leading and respected status as a voice on issues of data and privacy, we are frequently called upon to give expert evidence to parliamentary and government committees, including the European Parliament, the Council of Europe and the UN Office of the High Commissioner for Human Rights.

Software is what keeps our devices secure, functional, compatible with the latest apps, and protected against known security vulnerabilities. Out-of-date software on an otherwise functioning device can be a door to one's bank account or the intimacy of one's life, render a device unusable, or worst still endanger safety and life even. Such a risk is enabled by software support periods that are shorter than the product's usable life cycle, and an industry focused only on selling its latest products rather than providing long-term

software support for their older products. This is not a sporadic phenomenon; it is a practice deployed by most dominant actors in the digital markets for various categories of popular products. The text of the draft Regulation should thus be improved with amendments to ensure that current company practices do not result in serious harms for consumers or negatively impact devices' sustainability and digital innovation.

I. ENSURING LONG-TERM SECURITY UPDATE SUPPORT FROM DEVICE MANUFACTURERS

When purchasing devices and services, it is often unclear how long these will be supported with software updates. **PI's research illustrates how the current software support landscape is characterised by varying and inconsistent approaches to security updates, as well as by software support periods that differ based on product category and among the same connected devices.** [1] In addition, information about how long connected devices will be supported with either functionality or security updates, or both, is rarely provided to consumers at the point of purchase and will very often be missing from the companies' website. Even when this information is disclosed it is not always easily accessible to the average consumer. [2] **This practice allows manufacturers to sell devices with "out-of-date" software, often at a discount, at the expense of consumers' rights.**

Article 10(6) of the Draft Regulation imposes an obligation on manufacturers who place products with digital elements on the market to *"ensure that vulnerabilities of that product are handled effectively"* for the *"expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter"*. Likewise, paragraph 12 of the same article obliges manufacturers *"who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I"* to *"immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate"*.

1 PI, We looked into the software support practices for 5 of the most popular smart devices (and the results may disappoint you) (20 October 2022), https://privacyinternational.org/report/4965/we-looked-software-support-practices-5-most-popular-smart-devices-and-results-may

2 For a detailed overview of the software support practices of some of the most popular manufacturers of connected devices, see Annex A.

While such obligations to ensure that products with digital elements receive long term security software support should be welcomed, the text of the Draft Regulation fails to distinguish between the various categories of products with digital elements that currently exist on the market. **Instead, the Commission proposal adopts a blanket approach for all devices and merely obliges manufacturers to provide security updates only for a maximum of 5 years or even less should the expected lifespan of a device be shorter than this.** This is a serious shortcoming as it, first, allows manufacturers to stop supporting devices that are perfectly functional and still used by EU consumers for periods that are longer than 5 years, such as smartphones or personal computers, which can also often pass on to older generations, as well as various household appliances that have increasingly become 'smart' and are expected to last a lot more than five years. such as smart thermostats or smart fridges, washing machines and televisions. [3] Second, a 5-year maximum duration of security software support could adversely hamper innovation, competition, and device sustainability, by resulting in increased premature obsolescence and, accordingly, e-waste.[4]

3 A 2022 YouGov survey commissioned by PI shows that consumers expect their smartphones, computers, smart TVs and gaming consoles to receive security updates for a much longer period than what several manufacturers actually provide, leaving consumers with expensive tech that is vulnerable to malfunctions and third-party attacks, PI, Privacy International research shows that smart device security updates fail to meet consumers' expectations (20 October 2022), https://privacyinternational.org/press-release/4964/privacy-international-research-shows-smart-device-security-updates-fail-meet

4 Europe ranks first worldwide in terms of e-waste generation per capita (16.2 kg), so its mandated recycling schemes, however efficient, simply cannot keep up with the rate of new e-waste generation which is fuelled not just by increased consumption, but also by in-built short life cycles of devices (so called 'planned obsolescence') and few repair options, see Forti V., Baldé C.P., Kuehr R., Bel G. The Global E-waste Monitor 2020: Quantities, flows and the circular economy potential. United Nations University (UNU)/United Nations Institute for Training and Research (UNITAR), https://www.itu.int/en/ITU-D/Environment/Documents/Toolbox/GEM_2020_def.pdf

II. INCREASING TRANSPARENCY ABOUT THE HANDLING OF SOFTWARE VULNERABILITIES

We note that the Commission's proposal seeks to impose obligations on manufacturers to promptly notify the EU Agency for Cybersecurity (ENISA) of any actively exploited vulnerabilities contained in products with digital elements (Article 11). ENISA would in turn inform the market surveillance authority about the notified vulnerability (Article 11(1)).

Essentially this would mean that **member states might eventually be able to gain access to vulnerabilities that have not necessarily been fixed by the manufacturer.** It should be underlined that the draft Regulation **grants national market surveillance authorities sweep powers, which come without explicit safeguards to prevent them from stockpiling vulnerabilities at the cost of undermining IT security and data integrity.**

What past cyberattacks have underlined is that hoarding system vulnerabilities might have onerous consequences for citizens across the whole Union. [5] Furthermore, an April 2022 ENISA report on Coordinated Vulnerability Disclosure (CVD) Policies in the EU demonstrates that the current EU environment is characterised by fragmentation and non-consistent policies. Specifically, as the ENISA research shows, 19 member states do not have a CVD policy. [6] In March 2022, the European Parliament established a Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, [7] which rely on the

5 EU Agency for Fundamental Rights (FRA), Fundamental Rights Report 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf, page 161.

6 ENISA, Coordinated Vulnerability Disclosure Policies in the EU (April 2022), https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

7 European Parliament decision of 10 March 2022 on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee (2022/2586(RSO), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0071_EN.html

exploitation of vulnerabilities in IT devices and networks to access devices and exfiltrate data. But these same vulnerabilities can also be potentially exploited by anyone else who is aware of them, including criminals and foreign states. It should be underlined that at least 5 EU member states that have been reportedly involved in the use of Pegasus or other spyware, namely Bulgaria, Cyprus, Hungary, Poland, and Spain, [8] are also among the ones that have not implemented a formal policy regarding coordinated vulnerability disclosure, according to the aforementioned ENISA report.

Additionally, the draft Regulation needs to go further and ensure that any known vulnerability is immediately fixed and then publicly disclosed by device manufacturers as part of the product's change log or release notes. This would increase digital security and boost competition by enabling customers, other market participants, and the public to create a history of vulnerabilities and evaluate the long-term quality and trustworthiness of a software product on the EU market.

8 European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, Pegasus and surveillance spyware (In-Depth Analysis for the Pegasus Committee, May 2022).

III. EXPLICITLY EXCLUDING OPEN-SOURCE PROJECTS FROM THE SCOPE OF THE REGULATION

Free and open-source software (FOSS), such as openSSL and WordPress, has been crucial for digital innovation not only because many critical elements of the Internet rely on it to operate, but also because it has enabled several communities and researchers. [9] While the draft Regulation rightly seeks to exempt FOSS, Recital 10 and Article 3(3) suggest that certain FOSS projects might nevertheless be covered by the Regulation, and thus subject to the obligations it seeks to impose, because, for example, they might provide support services for a fee or they might receive donations. As a result, digital innovation would be significantly hampered as developers of open-source software outside the internal market might geographically restrict access to open-source code or even be discouraged from sharing their ideas. [10]

9 See Olaf Kolkman, The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem (Internet Society, 24 October 2022), https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem.

10 Ibid

IV. TABLE OF PROPOSED AMENDMENTS

Recital 10 In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions,	**Recital 10** In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions,
Recital 19 […] On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive [Directive XXX / XXXX (NIS2)]. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation […]	**Recital 19** […] On the basis of the information it gathers, ENISA should prepare and publish on its website a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive [Directive XXX / XXXX (NIS2)]. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. […]

Recital 34 To ensure that the national CSIRTs and the single point of contacts designated in accordance with Article [Article X] of Directive [Directive XX/XXXX (NIS2)] are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ENISA vulnerabilities that are being actively exploited. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should also consider disclosing fixed vulnerabilities to the European vulnerability database established under Directive [Directive XX/XXXX (NIS2)] and managed by ENISA or under any other publicly accessible vulnerability database.	**Recital 34** To ensure that the national CSIRTs and the single point of contacts designated in accordance with Article [Article X] of Directive [Directive XX/XXXX (NIS2)] are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should **take all reasonable steps necessary to fix vulnerabilities within 90 days and then notify fixed vulnerabilities** to ENISA. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should also consider ~~disclosing~~ **disclose** fixed vulnerabilities to the European vulnerability database established under Directive [Directive XX/XXXX (NIS2)] and managed by ENISA or under any other publicly accessible vulnerability database. **Once the vulnerability has been fixed, the manufacturer shall disclose it as part of the product's change log or release notes.**

Article 3(23) 'making available on the market' means any supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;	**Article 3(23)** 'making available on the market' means any supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge. **For the avoidance of doubt, the charging of a price to provide technical support for open-source software or the use of personal data for reasons relating to improving the security, compatibility or interoperability of the software shall not be deemed a commercial activity, whereas the bundling of free and open-source software with proprietary software shall be considered a commercial activity.**
Article 10(6) When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.	**Article 10(6)** When placing a product with digital elements on the market, and for the expected product lifetime or for a period of ~~five~~ **ten** years from the placing of the product on the market, whichever is ~~shorter~~ **longer**, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

Article 10(12) From the placing on the market and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.	**Article 10(12)** From the placing on the market and for the expected product lifetime or for a period of ~~five~~ **ten** years after the placing on the market of a product with digital elements, whichever is ~~shorter~~ **longer**, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate. _

Article 11(4) The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.	**Article 11(4)** The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident. **The manufacturer of the product with digital elements with vulnerabilities shall also take all reasonable steps necessary to fix the vulnerabilities within 90 days of becoming aware of them. In certain cases, the 90-day deadline may be extended but it should not exceed 6 months. Once the vulnerability has been fixed, the manufacturer shall disclose information about it as part of the product's change log or release notes.**
Article 49(2) Unless otherwise agreed upon by the market surveillance authorities involved, sweeps shall be coordinated by the Commission. The coordinator of the sweep may, where appropriate, make the aggregated results publicly available	**Article 49(2)** Unless otherwise agreed upon by the market surveillance authorities involved, sweeps shall be coordinated by the Commission. The coordinator of the sweep ~~may, where appropriate,~~ **shall** make the aggregated results publicly available.

Article 49(5) Market surveillance authorities may invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.	**Article 49(5)** Market surveillance authorities may invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps **only in cross border cases.**

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).