WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

STATEMENT

On the Commission 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

Berlin, 22 December 2022

With the European Cybersecurity Act in 2019, the European Union established a framework for the certification of digital products and services. This framework, while largely voluntary, was supposed to bolster the uptake of security mechanisms and schemes and increase the level of cybersecurity throughout the European Union. The now-proposed Cyber Resilience Act (CRA) builds upon the foundations of the Cybersecurity Act, adds additional clarity to the general European cybersecurity scheme, and further specifies security requirements for digital products.

eco – Association of the Internet Industry advocates for the enhancement of security in networks and services and welcomes the initiative as a further step towards achieving this goal. Responsibility for security in ICT products and services is a difficult task to allot, and eco believes that the provisions of the proposed Cybersecurity Act, in general, address the topic with the scrutiny and diligence required to strike a balance between the different actors and parties involved.

Close attention should be paid to the fact that many of the provisions of the CRA do not automatically create an enhanced level of cybersecurity. Rather, they require different actors within the field of cybersecurity to more closely document and evaluate their products and services. This creates an administrative overlay for companies, which must be balanced with the future increase in their cybersecurity practices and awareness. This will be of specific concern when it comes to managing the investment in and the requirements for open-source software.

In this context, eco would like to comment on the following topics arising from the proposed CRA:

- **On Article 2:**

The definitions, while generally sound, are a matter of concern for the developers of open-source software, who see a lack of distinction between open-source software distributed on a not-for-profit basis and commercial software. eco recommends exploring the further implications and harmful effects for the development of open-source software for deployment in the market on a not-for-profit basis.

- **On Article 4: Free movement**

The definition of "unfinished software" in Article 4(3) is not in line with the current status of product and software development. It specifically contradicts the premises and conditions for the deployment and use of open-source software. eco recommends further exploring the topic so as to avoid unintended detrimental effects on the European software industry.

- **On Article 6: Critical products with digital elements**

eco welcomes the approach the Commission set out in its draft for the CRA. However, the Internet industry advocates a more transparent and understandable approach when determining the respective role of products and services falling within the scope of critical products. This topic largely addresses the Commission's ability to pass delegated acts on certain topics, which – in eco's opinion – require a more exact definition in order to avoid legal uncertainty for companies placing software and products on the market. Providers of hardware, software and network operators should be able to rely on binding rules suited and intended for them and not run the risk of being subject to double regulation.

- **On Article 8: High-risk AI systems**

As stated on the comments on Article 6, eco hopes that legal clarity for ICT companies should be given the necessary consideration when drafting the CRA. As it is, high-risk AI systems are already covered through the European Commission's AI Act and an additional AI liability Act is also currently in preparation. eco would like to point out that this regulatory framework may be difficult to navigate. This applies especially to smaller companies which do not possess the resources to manage different, maybe even conflicting, requirements under various acts of legislation.

- **On Article 10: Obligations of manufacturers**

The obligations for manufacturers, while appearing proportionate and generally acceptable, raise the question of why the Commission decided to require manufacturers to address cybersecurity deficiencies for either the product lifecycle or for five years, whichever is shorter. The latter requirement may transfer responsibility for product and network safety from the manufacturer to the network operator. This could lead to a wide array of problems; ranging from questions on the activities network operators have to take in order to address problems arising from possible obsolescence after five years to liability questions. The Internet industry advocates – for reasons of clarity – that the responsibility for the security of a product should be throughout its lifecycle with the manufacturer and, after that, with the operators of the product in the knowledge that it is no longer supported.

- **On Article 11: Reporting obligations of manufacturers**

The reporting deadline of 24 hours stipulated in CRA Article 11 (1) for manufacturers who become aware that there are vulnerabilities in their products is, from eco's point of view, too tight. As the regulation states, any vulnerabilities should be reported without undue delay. This does, however, not preclude that it should be reported within 24 hours, which may lead to correction of reportings and thus create an administrative burden for manufacturers.

Additionally, eco regards the intended structure of the reporting mechanism as problematic. While NIS2 requires companies to report to their respective national authorities, the CRA foresees ENISA as the main recipient of such reports. eco recommends reviewing the provision in order to avoid complexity in the exchange of information for companies and administrations alike.

- **On Article 13: Obligations of importers**

The obligations placed on importers in Article 13 create ambiguity with the rules set out in the preceding articles of the regulation. While importers may well determine that a product they import possesses the required certificates, it is difficult, maybe even impossible, for them to establish whether the product is actually compliant with its certification. One can generally assume that importers have a vital interest in importing only certified goods, which can be deployed or placed on the market. Thus, a further specification requirement for importers to determine potential defects in products creates legal uncertainty for them. The provisions in Articles 13(3) and 13(6) should be carefully reviewed, and measures should be taken to clarify that shifts in liability do not arise from these provisions.

- **On Article 14: Obligations of distributors**

Corresponding with the criticism against Article 13, eco points out that the obligations for distributors similarly contradict the aim of the regulation to strike a balance between the responsibilities of manufacturers, distributors and users. The implementation of provisions that require distributors to become active in the field of identifying or removing vulnerabilities contradicts this aim and should not be required. eco recommends reviewing the respective provisions in Article 14 (4).

- **On Article 17: Identification of economic operators**

The provisions set out in Article 17 create reporting duties that are onerous from the point of view of the Internet industry. At the same time, they do not seem to contribute to any increase in cybersecurity. eco advocates a critical review of the

requirement to record and store information on the exchange of digital products and services with business customers. The requirement to be able to provide such information for ten years according to Article 17(2) is questionable and does not correspond with other provisions of this regulation. The Article also generally does not provide any limitations or binding safeguards on the reasons put forward by market surveillance authorities for requesting respective information. eco calls for a critical review of this provision.

- **On Article 42: Access to data and documentation**

While it is understandable that market surveillance authorities need information to conduct a proper evaluation of the conformity of a certain product, it should also be specified that the information gathered through such processes should be exclusively limited to said assessment. It should not be further disseminated or shared with other authorities for their respective purposes. eco would also like to point out that, very often, questions about patents and trade secrets may be involved in such an evaluation. For this reason, the assessment of conformity should be conducted in a closed environment.

- **On Article 52: Confidentiality**

Confidentiality is an important factor for manufacturers providing the European market with different products and services. Their intellectual property is at stake when they are subjected to evaluations on compliance with general security obligations. eco understands that information has to be shared by companies and manufacturers with market surveillance bodies so they can fulfil their functions properly. However, eco regards it as highly problematic that information may be disseminated by market surveillance bodies to other bodies and the European Commission as set out in Article 52 (2) without prior consultation of the company providing the respective information. The Internet industry requests that disclosure of information during conformity assessments, which basically implies “before entering the market”, should only occur after consultation with the companies involved and thus avoid reputational damage for companies undergoing security assessments.

Conclusion

The Cyber Resilience Act provides a solid framework for the future certification of digital products and services and, in general, allots responsibility to those actors that have the greatest influence over it. However, closer attention should be paid to provisions that counteract this approach and may create shifts in liability that may not be intended by the legislator and create uncertainty for operators of said products and services. Ambiguity in these provisions will not help increase

cybersecurity but may, in fact, prove counterproductive. This problem specifically affects network operators and providers of open-source software which is distributed on a not-for-profit basis.

Additionally, eco would like to raise the question of whether the amount of information to be shared is actually appropriate and whether more safeguards should be implemented in order to preserve trade secrets and intellectual property.

Lastly, eco appeals to the lawmakers to have a deeper look at the general legislative requirements in the field of conformity assessments in order to avoid double regulation. This can help create a level playing field for all market participants. More clarity about which companies and actors exactly are subject to the provisions of the CRA – and which fall under other regulations – is needed if the Cyber Resilience Act is to become a success.