POSITION PAPER

for the trilogue negotiations on the 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 November 2023

With both the Council and the Parliament having cleared the way for trilogue negotiations on the Cyber Resilience Act (CRA) on 19 July 2023, the proposed Regulation of cybersecurity requirements for networked products is now at the helm of the debate on increasing the level of safety in both products and services for customers and networks.

eco – Association of the Internet Industry would like to take the opportunity regarding the ongoing trilogue on the CRA to address a set of topics that should be further discussed while elaborating the new legislation. In this respect, eco's rationale is to create a legal framework which increases the security of both networks and products, while at the same time providing companies with applicable and comprehensible rules.

From the Internet Industry's perspective, in completing the CRA, the following aspects warrant closer examination:

- **Create comprehensible rules for Open Source Software developers**

eco would like to draw attention to the fact that the provisions of the CRA may jeopardise the development and deployment of Open Source Software in Europe. The provisions contemplated by the Commission proposal in Articles 2 and 4 are the main setback for Open Source Software developers. While the Parliament has addressed the challenges for Open Source Software developers, eco is of the opinion that the formulation of the LIBE Committee might not adequately deter questions on responsibility. It is anticipated that questions will also be placed on liability, and that the subjection of Open Source Software developers – who do not receive reimbursement for the development and deployment of their products – will be subjected to the provisions of the CRA. This means that the use and application of Open Source Software in the European market may deteriorate due to the reduced willingness to publish it. Additionally, the Open Source Community in Europe may encounter difficulties in finding partners for cooperation in an international, globalised software development environment. As the Council is currently not touching on this topic in any respect, in order to foster the development of Open Source Software, eco would recommend reviewing the respective Articles under this particular aspect, adding clarifications, and clearly delineating responsibilities to recital 10.

- **Proportionate rules for products with digital elements**

With the Commission’s proposal, a framework was set up in Article 6 to define critical products with digital elements. While this approach is not flawless, it has been vigorously addressed by both the Parliament and the Council. eco would like to emphasise that both the definition of critical products with digital elements and their respective rules should be understandable and proportionate. While the Council approach is set out to link the CRA closer with the European Cybersecurity Regulation ((EU) 2019/1020), the Parliament is adopting a different approach. This involves setting up an expert group on cyber resilience which shall support the Commission in working out delegated acts and further governing critical products with digital elements. In this context, eco welcomes the Parliament’s inclusive approach to governing cyber resilience. Setting aside the question as to whether existing bodies or organisations can fulfil this role, the basis for comprehensive rules for cyber resilience lies in dialogue with all actors included. This should, however, not discard the concern that a double Regulation may still be a problem for networked products and needs to be avoided. In this regard, in order to avoid duplications, the CRA should build on and align with the NIS2 Directive. This aspect should be given more attention in the ongoing trilogue.

- **Cybersecurity conformity governance scheme should not create ambiguity**

In Chapters III and IV, the CRA included an encompassing framework for the establishment of a governance scheme on assessing conformity complete with national authorities, alongside a competitive structure for conformity assessment. The Internet Industry would like to draw attention to the following concern: that the manner of organising conformity assessment may create a fragmentation in the internal market if there is no central authority working towards establishing a harmonised approach to assessing conformity with cybersecurity requirements at the European level. eco would welcome further clarification in the CRA on how this goal is going to be achieved in order to avoid market segmentation or fragmentation.

- **Responsibilities of manufacturers require more scrutiny**

The Parliament and the Council have concluded that the provisions and reporting obligations for manufacturers (Art. 10 & 11) should be adjusted. While the Parliament has set up a detailed reporting and early warning mechanism, the Council aims to identify all mobile devices individually. eco would like to reiterate that the obligations for manufacturers should be comprehensive as well as balanced. eco fears that the proposals from the Parliament and the Council may make these obligations a great bureaucratic burden for manufacturers and would like to restate that the Commission’s proposal was generally sound. A factor that was inadequately addressed was the question of responsibility transition after the end of the product lifetime. While it may be welcome to note that the Parliament’s proposal does offer additional evidence like source code and extends the general reporting obligation to ten years, the general problem is nonetheless not adapted, given that the transition of responsibility in the CRA has not been properly addressed. The Internet Industry would benefit from a clarification regarding at which point responsibility concerning the safe operation of a product with digital elements shifts from the manufacturer or vendor to the operator. What also should be clarified is the role of Open Source Software developers who are publishing their code without any form of reimbursement – including compensations other than monetary (e.g. personal) data.

- **Conclusion**

eco understands that the CRA is intended to increase the general level of cybersecurity throughout networks and systems, making the Internet safer. eco supports this goal and advocates for a consistent framework for cybersecurity in networked products, which includes manufacturers as well as importers or vendors and addresses their responsibilities and liabilities.

However, this framework should be proportionate for these actors and not create bureaucracy as an end in itself. Especially when it comes to the conformity assessment of networked products, eco is of the opinion that the path chosen by the trilogue partners falls short, since it does not address harmonisation of cybersecurity requirements in the digital single market. For the Internet Industry, this obstacle must be overcome in order for the CRA to become a success.

Additionally, the CRA should not obstruct the development and deployment of Open Source Software. eco understands that a comprehensive framework on cybersecurity includes the developers of Open Source Software. However, the provisions should not lead to disproportionate strains on these developers, and remedies must be found in order to allow these actors to participate in the market.

The CRA can only properly contribute to the governance of cybersecurity in Europe if these problems are collectively addressed in the ongoing trilogue.

<u>About eco:</u> With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.