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

STATEMENT

Call for Evidence for an Impact Assessment on the Cyber Resilience Act – Ref. Ares(2022)1955751

Berlin, 20. May 2022

The interplay of market mechanisms and state regulation form a specific peculiarity of European cybersecurity. With the NIS Directive from 2016 and the European Cybersecurity Act from 2019 in place, and a major revision of the NIS Directive currently being negotiated in trilogue, a major question in the field of cybersecurity regulation concerns how market-driven innovation, government-provided security schemes and protection of users and citizens in this field can interact with each other.

From the EU Commission's perspective, the upcoming Cyber Resilience Act is intended to be an important factor for the future interaction between digital companies and services, producers of hardware and equipment, users and citizens, and regulators. The Internet industry has advocated for striking a balance in the field where responsibilities and obligations are allocated to the different actors according to their abilities and liberties.

eco – Association of the Internet Industry has the following remarks on the Call for Evidence on the Cyber Resilience Act:

I. Problem the initiative aims to tackle

The Commission claims that many products are often placed on the market without "adequate cybersecurity safeguards" and further spells out several reasons as to why this occurs. In the first place, eco would like to point out that simply demanding "adequate cybersecurity safeguards" inadequately addresses the complexity of the cybersecurity environment. Trust services or critical infrastructures require different cybersecurity safeguards than home-computing applications or simple office environments. Striking a balance between these different fields – and identifying them in the first place – is a complex challenge that is not easy to address. Additionally, the Commission sets out that the main focus of this problem is allocated to vendors, which are also described very broadly. A vendor may in fact also be a trading company which does not have any influence over product design or security functions. Given the fact that information allocation in a dynamic ICT environment is different among various actors, this may lead to a different allocation of responsibility for existing cybersecurity deficiencies or the knowledge on these. From eco's point of view, a limitation of responsibility for lack of information may thus lead to a market disruption. Obligations should ideally lie with those actors in instances where there is the most potential to positively impact

cybersecurity through product design etc., with countermeasures therefore being most effective. eco understands that the Commission intends to regulate this unclear field. However, eco would like to point out that a one-size-fits-all solution will most likely not serve industry or traders' needs. It could also lead to a complex, multi-layered reporting system that would not increase the level of information for consumers or add to the Commission's defined goal of adding to adequate cybersecurity safeguards. eco advocates for a balanced and unbureaucratic liability system, which should cover many cases in a comparable way and which would allocate responsibility for cybersecurity to the different actors in their respective roles. This may include special regulation for certain aspects.

II. Objectives and policy options

Despite a broad variety of legal acts in different fields, the legislative framework for the EU's Digital Market often remains fragmented, with gaps in the digital value chain not being addressed. The discussion about the need and content of a Cyber Resilience Act could provide an opportunity to harmonize European cybersecurity obligations and achieve more legal consistency between national and European levels. That being said, eco supports the goals set out by the Commission to enhance cybersecurity in order to service specific risks throughout a product's life cycle. As previously stated, this goal is often not easily reached due to the nature of interconnected services and products.

Regarding the five different policy options the Commission has proposed, eco acknowledges that several obligations for software and IT are already in place and are currently being implemented in the EU's Member States. Additionally, the Cybersecurity Act and the NIS Directive are addressing issues such as definitions of products and services, their level of criticality and the respective certification. This highlights a problem emerging from the history of the European cybersecurity regulation; a problem which to some extent was initiated in the plan for the Cyber Resilience Act, but which relates even more to the fact that this act represents the third cybersecurity regulation since 2019 (not including general liability rules). Along with the fact that the national regulation accompanies or even goes beyond these European rules, this leads to a high frequency of new obligations that companies are subjected to. This proves to be a growing problem for digital companies in Europe.

From this point of view, eco would see another horizontal regulation adding new requirements to cybersecurity management as problematic, given that many fields are already covered with a sector-specific regulation or general liability obligations. A horizontal regulation that would integrate other regulations and thus make separate ones obsolete might prove beneficial for clarity and legal certainty. eco supports closing existing liability gaps where necessary and streamlining and harmonizing cybersecurity requirements through regulation where applicable. From this point of view, eco would see another horizontal regulation which adds new

requirements to cybersecurity management as problematic, since many fields are already covered with sector-specific regulations or general liability obligations.

III. Conclusion

Following these considerations, eco cannot vouch for one of the proposed policy options and instead recommends a review of the existing cybersecurity regulatory framework and an endeavour to harmonize the regulations through closing regulatory or liability gaps. The framework to be created through this approach would be robust and flexible and would contribute to an enhanced level of cybersecurity, while avoiding bureaucratic shortfalls.

--

About eco: With more than 1,000 member companies, eco is the largest Internet industry association in Europe. Since 1995, eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust, and ethically oriented digitalisation. That is why eco advocates for a free, technology-neutral, and high-performance Internet.