ESBG response to the EC public consultation on the Cyber Resilience Act

Position – Executive Summary

May 2022

ESBG Transparency Register ID 8765978796-80

On 18 May 2022, ESBG submitted its position to the European Commission's public consultation on the Cyber Resilience Act. All feedback received will be taken into account as the Commission further develops and fine-tunes this initiative.

In March 2022, the European Commission launched a public consultation to gather views from a wide range of stakeholders to help shaping the Cyber Resilience Act, a regulation on horizontal cybersecurity requirements for digital products and ancillary services.

Digital products and ancillary services create opportunities for EU economies and societies. However, they also lead to new challenges – when everything is connected, a cybersecurity incident can affect an entire system, disrupting economic and social activities. The initiative for a Cyber Resilience Act aims to address market needs and protect consumers from insecure products by introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services.

ESBG submitted its position to the European Commission's public consultation on the Cyber Resilience Act on 18 May. Feedback received will be taken into account as the Commission further develops this initiative, that is tentatively scheduled for Q3 of 2022. Input will help the Commission analyse cybersecurity-related problems associated with the digital products markets, explore possible ways forward and assess the impact of different types of interventions. ESBG provided the Commission with its position on the following aspects: I) Cybersecurity of digital products and the users of digital products; II) Improving the cybersecurity of digital products; and III) Stakeholder impact of potential regulatory measures.

Our position

ESBG welcomes the European Commission's Cyber Resilience Act as the level of risk of cybersecurity incidents affecting digital products has increased during the last five years. The overall level of cybersecurity of digital products marketed in the European Union could be improved. Subjecting certain products marketed in the Union to cybersecurity requirements would be effective (e.g. hardware or software products subject to higher cybersecurity risks).

Moreover, ESBG members find a self-declaration as a way for hardware manufacturers and software developers to demonstrate compliance with security requirements insufficient. It would be more valuable to have the opinion of a third party based on a control framework.

READ THE FULL POSITION PAPER

Your contact: Janine Barten – janine.barten@wsbi-esbg.org www.wsbi-esbg.org