ESBG response to the European Commission's call for feedback on the Cyber Resilience Act

Position – Executive Summary

November 2022

ESBG Transparency Register ID 8765978796-80

On 14 November 2022, the Joint Office submitted the ESBG position to the European Commission's call for feedback on the Cyber Resilience Act. All feedback received will be summarised by the Commission and presented to the Parliament and the Council with the aim of feeding into the legislative debate.

Guaranteeing the cyber-resilience of hardware and software products

The European Savings and Retail Banking Group welcomes the European Commission's proposal for a Cyber Resilience and supports the goal of only having secure software on the internal market. Savings and retail banks, as users of the products that fall under the scope of application of this regulation, support the initiative to guarantee the cyber-resilience of hardware and software products that can be and are acquired by the entities. A cross-sectorial legal framework has not been established so far to guarantee the cyber-resilience of hardware and software products with digital elements and obliges manufacturers, importers and distributors to comply with essential design, development and production requirements.

Existing vertical initiatives

However, there are vertical initiatives that already regulate the cyber-resilience of hardware and software products used by certain sectors. This is the case of the Digital Operational Resilience Act (DORA) for the financial sector; a regulatory framework specifically designed and developed to ensure the digital operational resilience of the financial sector.

A clear scope-statement

Regarding the scope, we therefore propose the Commission makes a clear scope-statement that would dissolve any uncertainty whether the software developed, operated, and/or marketed by financial institutions (e.g., through Apple, Google Playstore, or through its own channels) is in scope of this Act. The European Savings and Retail Banking Group believes that the Cyber Resilience Act leaves much room for interpretation regarding its scope of applicability. Extending its scope to products manufactured by credit institutions may place additional burdens onto banks, on top of the already existing tight regulatory corset.

READ THE FULL POSITION PAPER HERE

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