POSITION PAPER

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

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

November 2022

ESBG

1. GENERAL INFORMATION

On 15 September 2022, the European Commission published a proposal for a Cyber Resilience Act, which is supposed to protect consumers and businesses from products with inadequate security features. The Cyber Resilience Act introduces mandatory cybersecurity requirements for products with digital elements, throughout their whole lifecycle. It will ensure that digital products, such as wireless and wired products and software, are more secure for consumers across the EU: in addition to increasing the responsibility of manufacturers by obliging them to provide security support and software updates to address identified vulnerabilities, it will enable consumers to have sufficient information about the cybersecurity of the products they buy and use.

On 19 September 2022, the European Commission opened a possibility to provide feedback on the proposed Cyber Resilience Act for a minimum period of 8 weeks until 13 December 2022 (midnight Brussels time). All feedback received will be summarised by the European Commission and presented to the European Parliament and Council with the aim of feeding into the legislative debate. Feedback received will be published on the consultation website of the European Commission and therefore must adhere to the feedback rules.

2. FEEDBACK

The European Savings and Retail Banking Group (ESBG) welcomes the European Commission's proposal for a Cyber Resilience Act (from now on referred to as CRA) and supports the goal of only having secure software on the internal market.

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 this type of product with digital elements and obliges manufacturers, importers and distributors to comply with essential design, development and production requirements.

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.

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.

We request such a statement for the following reasons:

Unclear scope of applicability

- While first having gained the impression the CRA wants to address Internet of Things-products and certain critical IT-infrastructure assets, a closer inspection of the CRA seems to paint quite a different picture:
    - Art 2(1) states the CRA "*applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network*";
    - Art 3(1) qualifies "*products with digital elements*" as "*any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately*";
    - Art 3(6) qualifies "*software*" as "*the part of an electronic information system which consists of computer code*";
    - Art 3(9) qualifies "*electronic information system*" as "*any system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data*".

- With that in mind, virtually any app downloaded from an app-store could be subject to the CRA, because the app:

    - consists of computer code (Art 3(6));
    - is part of (installed on) an electronic equipment that is capable of processing data, i.e., a smart phone, (Art 3(6), 3(9));
    - will within its reasonably or foreseeable use connect to a network, i.e., internet, (Art 2(1)).

- The same is true for basically any other piece of software on the industrial or consumer market.

- The examples in Annex III do not help narrowing down the scope, because Annex III merely lays down what qualifies as "*Critical Products with Digital Elements*". This means that any products not mentioned in Annex III could still be subject to the general obligations of the CRA.

- While appreciating the goal of only having secure software on the internal market, we need clarification and guidance on the CRA's scope of application. For us, it remains unclear whether the EU indeed aims at regulating any and all pieces of software and hardware that may be connected to a network (e.g., online banking apps, ATMs).

The scope of the proposed Cyber Resilience Act needs to be specified.

- Recital 2 of the CRA states that one of its objectives is to create conditions to allow users to take cybersecurity issues into account when selecting and using products with digital elements. For this reason, **the CRA must apply exclusively to hardware and software products acquired by end users** - whether consumers or companies -, capable of being chosen or selected among different available options.

- Article 1 (a) of the proposed CRA states that it establishes rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products. Article 2.1, which establishes the scope of application of the Regulation, must include this condition, stating expressly the fact that it only applies to **products "placed on the market" and acquired by the user**. In this sense, we propose the following wording: *"This Regulation applies to products with digital elements placed on the market and acquired by the user – both consumer or company - whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network*".

Article 2 must expressly exclude from the scope of application of the Regulation products with digital elements manufactured, imported or distributed by financial entities.

- DORA establishes a regulatory framework specifically designed and developed to guarantee the digital operational resilience of the financial sector. In order **to avoid duplicating procedures and reporting obligations**, the proposed CRA must expressly exclude entities regulated by DORA from its application.

- The financial sector already has several cybersecurity and resilience layers and procedures, being one of the best prepared sectors in these terms. **Adding new obligations through the CRA for financial institutions will not help them achieve the objectives pursued, but it will involve duplicating processes, greater investment in resources, ambiguity, confusion and risk of incompatibility and inconsistencies**.

- As the CRA does, **DORA aims to guarantee that hardware and software systems operate without vulnerabilities in the financial sector**, including adequate obligations to guarantee cybersecurity from design, compliance with minimum security requirements, disclosure of information, evaluation of risks, the registration and notification of incidents to authorities, the correction of detected vulnerabilities and the management of risks derived from third parties, among others.

- Article 2.4 of the proposed Regulation establishes the rules that apply in the event that there are regulations that already regulate the requirements that address the same risks addressed by the CRA. However, this provision is ambiguous and confusing. In order to guarantee **legal certainty**, the express exclusion of financial entities from the application of the CRA is necessary.

Exemption for Banking Software

- If the CRA were to lay out a broad scope of applicability (as argued above), we still see products manufactured by the banking industry as being out of scope of the CRA.

- Art 2(4) states the following:

  "*The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded, where:*

  (a) such limitation or exclusion is consistent with the overall regulatory framework applying to those products; and

  (b) the sectoral rules achieve the same level of protection as the one provided for by this Regulation.

  The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend this Regulation specifying whether such limitation or exclusion is necessary, the concerned products and rules, as well as the scope of the limitation, if relevant."

- Credit institutions are already subject to DORA, NIS2, and PSD2, which already introduce certain default security standards to our products.

- Still, we believe that it is up to the European Commission to decide whether this is the case (by adopting delegated acts).

The presumption of compliance with the essential requirements established in article 18.3 must be based on the EU certification of implemented processes, not specific products.

- A certification for each product does not provide greater guarantees, but it does add inefficiency and slowness to the processes.

3. CONCLUSION

In conclusion, the European Savings and Retail Banking Group believes that the CRA 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.

About ESBG (European Savings and Retail Banking Group)

ESBG is an association that represents the locally focused European banking sector, helping savings and retail banks in 17 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 885 banks, which together employ 656,000 people driven to innovate at 48,900 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion billion in corporate loans, including SMEs, and serve 163 million Europeans seeking retail banking services. ESBG members commit to further unleash the promise of sustainable, responsible 21st century banking. Learn more at www.wsbi-esbg.org.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG. November 2022.