Position paper

of the Association of German Banks on the Cyber Resilience Act

7 March 2025

Lobby Register No R001458
EU Transparency Register No 0764199368-97

Bundesverband deutscher Banken e.V.
Burgstraße 28
10178 Berlin | Germany
Telephone: +49 30 1663-0
www.bankenverband.de

USt.-IdNr. DE201591882

The German private banks fully recognize that the Cyber Resilience Act will enhance cybersecurity standards of products that contain a digital component, requiring manufacturers and retailers to ensure cybersecurity throughout the lifecycle of their products from 2027 onward.

Therefore, we welcome rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products using essential cybersecurity requirements for the design, development and production of products with digital elements, and by establishing obligations for economic operators in relation to those products with respect to foster cybersecurity.

The scope of the Cyber Resilience Act applies to all products connected directly or indirectly to another device or network except for specified exclusions such as certain open-source software or services products that are already covered by existing rules.

This means that the Cyber Resilience Act as horizontal product-regulation rightfully recognises that it co-exists in a broader landscape of cybersecurity policies and that cybersecurity may already be regulated by sector-based policies or product-specific rules, e.g. by NIS 2 or by the Digital Operational Resilience Act (DORA) as lex specialis to NIS 2.

Today the Cyber Resilience Act contains five explicit exemptions in Article 2 (2) to 2 (4). Those exemptions apply today to products with digital elements that are subject to specific legal acts (e.g. for medical devices) or to certified products.

To ensure that the CRA remains future-proof and does not create additional bureaucratic burden, Article 2 (5) also contains an opening clause that would allow for a limitation or an exclusion for products "covered by other Union rules laying down requirements that address all or some of the risks covered by the essential cybersecurity requirements set out in Annex I" when (i) such limitation or exclusion is consistent with the overall regulatory framework that applies to those products; and (ii) the sectoral rules achieve the same or a higher level of protection as that provided for by this Regulation.

We are of the opinion that EU-wide by Financial Sector distributed digitalized financial products (e.g. mobile payment applications, payment cards, banking apps for servicing payment accounts, Automated Teller Machines for making cash disbursements and Point-of-Sale-terminals for accepting card payments) are eligible for such a limitation or exclusion given in Article 2 (5).

This paper outlines how the Digital Operational Resilience Act (DORA) as the overarching framework for the Financial Sector fulfils the requirement of the opening clause and would qualify for a respective Delegated Act by the European Commission.

o Even though DORA is not product-specific regulation, it requires financial institutions to establish an end-to-end framework for Information and Communication Technology (ICT) systems and assets.

o Applicable requirements cover the whole lifecycle of those ICT systems, from development, to implementation, ongoing application/ use and decommissioning. Throughout the whole lifecycle, DORA mandates – in a risk-based manner – documentation, monitoring, Vulnerability and patch management, incident identification, handling and reporting, as well as testing. Also, it sets more broadly requirements around the governance of ICT risk management and strategy.

o Despite the fact that DORA is not product-specific, the customer focus is addressed, too and is equally protected by DORA. DORA's overarching perspective goes way beyond the process of bringing a new product to market, as internal processes and systems are strictly scrutinised by supervisors to reduce and mitigate risks for the financial institution, customer assets and financial stability. Communication strategies for incidents are an integral part of the framework overall and create awareness with customers as appropriate and necessary.