The European Commission's work programme for 2022, released on 19 October 2021, announced a proposal on a European Cybersecurity Resilience Act (legislative) that is expected to be published in Q3 2022. As the Commission's President Ursula von der Leyen stated in her State of the Union Address in September 2021, the Act seeks to establish **common cybersecurity rules for digital products and associated services that are placed on the market across the European Union.** She also underlined that the EU should strive to become a leader in cybersecurity.

The Commission published in March 2022 a call for evidence for an impact assessment and a public consultation to gather views on existing problems and on possible policy options for such an initiative. According to the Commission, in a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain. This can lead to severe disruption of economic and social activities or even become life threatening. The lack of appropriate security in digital products and ancillary services is one of the main avenues for successful attacks.

When placing digital products or services on the market, vendors (e.g. hardware manufacturers, software developers, distributors and importers) may not put in place adequate cybersecurity safeguards. The current EU legislation covers only certain aspects linked to the cybersecurity of tangible digital products and, where applicable, embedded software concerning these products. The EU regulatory framework on products (e.g. the General Product Safety Directive and the Machinery Directive, both currently under review) does not prescribe specific cybersecurity requirements, e.g. covering the whole life cycle of a product. In addition, the existing framework does not cover all types of digital products.

The Cyber Resilience Act with horizontal cybersecurity requirements would aim to: (i) streamline and supplement existing rules; and (ii) prevent further fragmentation of cybersecurity requirements for digital products and ancillary services in the internal market, at both national and EU level.

The results of these consultations will feed into the Commission's proposal for a European Cybersecurity Resilience Act. The Cyber Resilience Act will complement the existing EU legislative framework, which includes the Directive on the security of Network and Information Systems (NIS Directive) and the Cybersecurity Act, as well as the future Directive on measures for high common level of cybersecurity across the Union (NIS 2).

BIPAR will be monitoring the legislative process in relation to the Cyber Resilience Act and will examine how its horizontal requirements could interact with sector-specific rules, for example the Digital Operational Resilience Act for the financial sector.