Digitalisation - European Cybersecurity Strategy

Why does it matter to intermediaries?

The EU Cybersecurity Strategy is an initiative aimed at building resilience to cyber threats through the Union and ensuring that citizens and businesses benefit from trustworthy digital technologies. In order to implement this strategy, the European legislators are working on several legislative proposals. The **Cyber Resilience Act** seeks to establish common cybersecurity rules for digital products and associated services that are placed on the market across the EU. It will complement the **Directive on measures for high common level of cybersecurity across the Union (NIS2).** The **Cyber Solidarity Act** aims to improve the preparedness, detection and response to cybersecurity incidents across the EU.

State of play

The Cyber Resilience Act

On 15 September 2022, the European Commission adopted a proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (the "Cyber Resilience Act"). On 30 November 2023, after three trilogues, the Council's Presidency and the European Parliament's negotiators reached a **provisional agreement** on the proposed Cyber Resilience Act.

This new Regulation introduces EU-wide cybersecurity requirements for the design, development, production and making available on the market of hardware and software products, to avoid overlapping requirements stemming from different pieces of legislation in EU Member States. It will apply to all products that are connected either directly or indirectly to another device or to a network. There are some exceptions for products for which cybersecurity requirements are already set out in existing EU rules, for example medical devices, aeronautical products and cars. The Regulation aims at allowing consumers to take cybersecurity into account when selecting and using products that contain digital elements, making it easier for them to identify hardware and software products with the proper cybersecurity features.

The provisional agreement maintained the general thrust of the Commission's proposal, namely as regards:

- rules to rebalance **responsibility** for compliance towards manufacturers, who must meet certain obligations such as providing cybersecurity risk assessments, issuing declarations of conformity, and cooperating with the competent authorities,
- **vulnerability handling processes** for manufacturers to ensure the cybersecurity of digital products, and obligations for economic operators, such as importers or distributors, in relation to those processes,
- measures to improve **transparency** on the security of hardware and software products for consumers and business users,
- a **market surveillance** framework to enforce the rules.

However, the co-legislators proposed various adjustments to parts of the Commission's proposal, mainly with regard to:

- the **scope** of the proposed legislation, with a simpler methodology for the classification of digital products to be covered by the new Regulation,
- the determination of the expected **product lifetime** by manufacturers: while the principle remains that the support period for a digital product corresponds to its expected lifetime, a support period of **at least five years** is indicated, except for products which are expected to be in use for a shorter period of time,
- the **reporting obligations** regarding actively exploited vulnerabilities and incidents: the NCAs will be the initial recipients of such reports but the role of the EU agency for cybersecurity (ENISA) is strengthened,
- the **new rules will apply three years** after the law enters into force.
- **additional support measures for small and micro enterprises** have been agreed, including specific awareness-raising and training activities, as well as support for testing and conformity assessment procedures.

The Cyber Solidarity Act

On 18 April 2023, the Commission adopted its proposal for a Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (the "Cyber Solidarity Act"). On 6 March 2024, the Council's Presidency and the Parliament's negotiators reached a **provisional agreement** on this Act.

The new Regulation establishes EU capabilities to make Europe more resilient and reactive in front of **cyber threats**, while strengthening cooperation mechanisms. It mainly aims to:

- support detection and awareness of significant or large-scale cybersecurity threats and incidents,
- bolster preparedness and protect critical entities and essential services, such as hospital and public utilities,
- strengthen solidarity at EU level, concerted crisis management and response capabilities across Member States,
- contribute to ensuring a safe and secure digital landscape for citizens and businesses.

To detect major cyber threats quickly and effectively, the new Regulation establishes a **"cyber security alert system"**, which is a pan-European infrastructure composed of national and cross-border **cyber hubs** across the EU. These are entities in charge of sharing information and tasked with detecting and acting on cyber threats. They will strengthen the existing European framework and in turn, authorities and relevant entities will be able to respond more efficiently and effectively to major incidents.

The new Regulation also provides for the creation of a **cybersecurity emergency mechanism** to increase preparedness and enhance incident response capabilities in the EU. It will support:

- preparedness actions, including testing entities in highly critical sectors (healthcare, transport, energy, etc.) for potential vulnerabilities, based on common risk scenarios and methodologies,
- a new EU cybersecurity reserve consisting of incident response services from the private sector ready to intervene at the request of a Member State or EU institutions, bodies, and agencies as well as associated third countries in case of a significant or large-scale cybersecurity incident,
- mutual assistance in financial terms.

Finally, the new Regulation establishes an **evaluation and review mechanism** to assess, amongst others, the effectiveness of the actions under the cyber emergency mechanism and the use of the cyber security reserve, as well as the contribution of this Regulation to strengthening the competitive position of the industry and service sectors.

The Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

The NIS2 Directive entered into force on 16 January 2023. It replaced the Directive on security of network and information systems (the NIS Directive) and improves the resilience and incident response capacities of both the public and private sector and the EU as a whole.

The NIS2 Directive is a framework containing general measures to boost cybersecurity through the EU. It applies to both public and private essential and important entities that provide their services or carry out their activities within the Union. The sectors to which the NIS2 Directive apply are listed in the Annex to the Directive and include the banking sector (and in articulation credit institutions) and the financial market infrastructures sector (and in particular operators of trading venues under MiFID II and Central Counterparties under EMIR). **Insurance intermediaries and financial advisers are not mentioned in the Annexes (but this is a minimum harmonisation Directive, meaning Member States may choose to extend its scope of application).**

Member States have to adopt and publish the measures necessary to comply with the NIS2 Directive by 17 October 2024. They must apply these measures from 18 October 2024.

BIPAR's position / key messages

BIPAR supports the initiative to build cyber resilience and cooperation across the Union. It highlighted the need for the emerging frameworks to take into account pre-existing sector-specific rules (for instance, the Digital Operational Resilience Act for the financial sector) in order to avoid duplication of obligations or fragmentation of the framework.

Next steps

The Cyber Resilience Act: the provisional agreement was approved by the Parliament as a whole on 12 March 2024. The text still needs to be formally adopted by the Council before it can enter into force.

The Cyber Solidarity Act: in March 2024, the Council's COREPER agreed on the final compromise text and announced it would approve the text if the Parliament's plenary vote would not change it anymore. In April 2024, the Parliament voted on the agreement reached in negotiations with the Council. The agreement will now have to be formally adopted by the co-legislators. It will then be published in the EU's Official Journal and will enter into force 20 days after this publication.

BIPAR will continue to follow the procedures regarding the adoption of the Cyber Resilience Act and the Cyber Solidarity Act and to assess the impact these texts might have on our sector.

Links

- EU Cybersecurity Strategy
- Cyber Resilience Act
- NIS 2 Directive
- Proposed Regulation on the Cyber Solidarity Act
- EP document on Cyber Solidarity Act
- EU Cyber Solidarity Act Factsheet
- Cyber Solidarity Act: Council's text