Presentation of the Cyber Resilience Act proposal

15 September 2022

EUROSMART
The Voice of the Digital Security Industry

Cyber Resilience Act proposal: Scope

- "[P]roducts with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network."
- Not covered:
  - ❖ Motor vehicles and trailers, medical devices, certified aircrafts, military or national security equipment, free and open source software
- Application of the Regulation **may be limited or excluded (TBD via delegated acts) in the case of products covered by sectoral rules where**:
  - ❖ such limitation or exclusion is consistent with the overall regulatory framework applying to those products

  AND
  - ❖ sectoral requirements achieve the same level of protection

Cyber Resilience Act proposal: Basic principles

- **Products with digital elements shall only made available on the market if**:
  - they comply with essential requirements of Section 1 Annex I and they are properly installed, maintained used, updated if needed
  - the process put in place by the manufacturer complies with Section 2 of Annex I (= vulnerability handling requirements)
- CE marking to indicate that these products comply with the Regulation
- Free movement for products that comply with the requirements

Cyber Resilience Act proposal: Different risk categories

- **Product with digital elements**
  - Internal control procedure is possible

- **Critical product with digital elements** (list in Annex III): class I (less critical) and class II (more critical)
  - Subject to stricter conformity assessment procedures involving a notified body (EU type examination or full quality assurance, as described in Annexe VI)

- **Highly critical products with digital elements** (Commission to define them via delegated acts):
  - They must be certified with a European cybersecurity certification scheme

→ In all cases, obligation for the manufacturers to perform a cyber risk assessment and include it in the technical documentation

Cyber Resilience Act proposal: Interaction with sectoral legislation

- Products covered by the **AI Act** or the **Machinery Regulation**: if they comply with the Cyber Resilience Act, then they shall be deemed in compliance with the cybersecurity requirements from the AI Act or the Machinery Regulation.
- Requirements of the Cyber Resilience Act aligned with relevant cyber provisions from **RED. Possibility to rely on ongoing RED standardisation work.**
- **eIDAS II**: issuers of Wallets shall ensure that their products (Wallets) comply with both the horizontal requirements and the cybersecurity requirements from eIDAS II. Certification of the Wallet via European cybersecurity certification scheme can demonstrate compliance with both legislations.
- **European Health Data Space Regulation**: systems must comply with both texts.

Cyber Resilience Act proposal: Cybersecurity requirements

(for exhaustive list see Section I Annex I)

- Appropriate level of cybersecurity based on the risks
- Products delivered without any known exploitable vulnerabilities
- Secure by default configuration
- Access control (authentication, identity management system etc.)
- Encryption of data
- Minimisation of data (only process the relevant data)
- Protection against denial of service attacks
- Limit attack surface, including external interfaces
- Security updates

Cyber Resilience Act proposal: Vulnerability handling requirements

(for exhaustive list see Section 2 Annex I)

- Identify and document vulnerabilities and components
- Address and remediate vulnerabilities without delay, including by providing security updates
- Effective and regular test and reviews of the security of the product
- Publicly disclose information about fixed vulnerabilities
- Policy on coordinated vulnerability disclosure

Cyber Resilience Act proposal: Reporting obligations

- Notification without delay (24h max) to ENISA of any actively exploited vulnerability. ENISA to forward the notification to the relevant national CSIRT.

- Notification without delay (24h max) to ENISA of any incident having impact on the security of the product. ENISA to forward the notification to the relevant national SPOC.

Cyber Resilience Act proposal: Harmonised standards

Presumption of conformity with Annex I for products and processes that are:

- in conformity with harmonised standards published in the Official Journal of the EU
- in conformity with common specifications
- certified pursuant to a European cybersecurity certification scheme (COM to determine whether the certificate eliminates the obligation of third party conformity assessment in the case of critical products)

In the case of critical products class I, presumption of conformity means that the products do not have to undergo the planned conformity assessment procedure involving a notified body.

Cyber Resilience Act proposal: Penalties for non-compliance

- **Non compliance with Annex I (cybersecurity and vulnerability handling requirements)**:
  administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 2.5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher

- **Non-compliance with any other obligations under this Regulation**:
  administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher

- **Supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request**:
  administrative fines of up to 5 000 000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher

Cyber Resilience Act proposal: Timeline

- Proposal will go through the ordinary legislative procedure (examination by the Council and the European Parliament).

- After entry into force of the Regulation, stakeholders will have 24 months to conform with the Regulation, except for the reporting obligation that should be implemented 12 months after entry into force.

- Transitional measures foreseen in Article 55.