April 2022

Position on the upcoming Cyber Resilience Act

Using what we have – placing the Cybersecurity Act at the forefront of EU cybersecurity legislation

To date, the EU is lacking an all-encompassing approach to cybersecurity. Cybersecurity provisions in current legislation are either limited to specific product groups or are only applicable on a voluntary basis. The EU Commission has recognized this significant regulatory gap and announced to propose a Cyber Resilience Act (CRA) in the third quarter of 2022. Among the options considered is a horizontal regulatory intervention introducing cybersecurity requirements for a broad scope of tangible and non-tangible digital products and ancillary associated services.

The TÜV Association welcomes the Commission's intention of establishing binding cybersecurity requirements for a broad range of products and services. However, instead of developing new and detailed horizontal cybersecurity requirements in the CRA as such, the EU legislator should built upon the existing EU cybersecurity framework. With the Cybersecurity Act (CSA)[1] adopted in 2019, there is a highly suitable regulation already in place that establishes comprehensive cybersecurity requirements for products, services and processes through its cybersecurity certification schemes. The only flaw is its voluntary character. Therefore, the CRA should make the CSA schemes, together with their associated assurance levels and conformity assessment procedures, legally binding. This approach will lead to a swift adoption of cybersecurity provisions without creating overlapping or diverging requirements.

The value of the Cybersecurity Act

- **Scope: a comprehensive cybersecurity framework**. The CSA establishes a cybersecurity certification framework for products, services and processes. Its scope thus goes beyond NLF-based product legislation by equally covering non-tangible products and ancillary associated services. Cybersecurity certification schemes can be developed for different areas ranging from consumer IoT devices over cloud services to 5G networks. Applying the CSA schemes allows using the existing framework without creating overlapping or diverging requirements, thus fully following the EU's better regulation principles.
- **Risk-based approach: graduated requirements and conformity assessment procedures.** The cybersecurity certification schemes comprise three assurance levels that prescribe the level of protection to be achieved: basic, substantial and high. The higher the assurance level, the more comprehensive the cybersecurity requirements and the corresponding conformity assessment procedures. While a self-assessment is possible for the assurance level basic, a certification by an independent accredited third party or a public authority is required for the levels substantial and high. This approach properly implements the precautionary principle.
- **Compatibility: key structural elements of the New Legislative Framework included.** The CSA is consistently compatible with existing EU legislation, as it shares key structural elements with the New Legislative Framework: the risk-based approach, the risk-adequate use of conformity

[1] Regulation (EU) 2019/881

assessment procedures, the presumption of conformity, the incorporation of harmonised standards as well as the instrument of accreditation for conformity assessment bodies. It is therefore well-suited to form the regulatory core of the CRA.

- **Governance: well-established institutions and structures**. The CSA has set up a well-established governance process with ENISA taking the lead as responsible agency for the development of the cybersecurity certification schemes. Stakeholder participation is properly ensured through the Stakeholder Cybersecurity Certification Group and the European Cybersecurity Certification Group.
- **Timeframe: several schemes in process.** ENISA is currently developing three cybersecurity certification schemes, notably a scheme for common criteria[2], 5G[3] and cloud services[4], which are expected to be published soon. Further schemes are already envisaged, including schemes for IoT consumer products and for IoT industrial products. Applying the CSA schemes allows a swift adoption of cybersecurity requirements to be complied with.

Policy recommendation: making the schemes of the Cybersecurity Act binding through the Cyber Resilience Act

- **Formulate only the overarching cybersecurity requirement in the CRA:** As regards cybersecurity requirements, the CRA should only formulate the basic provision to ensure a risk-adequate protection (robustness) against cyberattacks. It is to be applied to all harmonised and non-harmonised tangible and non-tangible digital products and ancillary associated services covered under this act.
- **Make the CSA scheme binding through a direct reference clause in the CRA:** For the detailed cybersecurity requirements, the CRA should directly refer to the CSA schemes by making their application mandatory for the respective group (e.g. consumer IoT devices, cloud services, 5G networks etc.). A general reference clause could be used for that.
- **Include a conflict-of-law rule**: The CRA should include a general conflict-of-law rule to avoid overlaps or diverging cybersecurity requirements between the CRA and sector specific legislation[5]. If the CSA and its schemes stipulate more stringent cybersecurity requirements than the sector-specific harmonisation legislation, the schemes should take precedence.

Suggested wording for the key provision of the Cyber Resilience Act:

"The product, ICT product, ICT service or ICT process shall be constructed, designed or built in such a way that it offers risk-adequate protection (robustness) against cyber-attacks, i.e. in particular that a cyber-attack on the ICT product, ICT service or ICT process must not impair the legal rights of users or third parties, in particular the protection of life and limb, including privacy. Within this, the specifications of the respective relevant schemes of the CSA including their risk assessment level must be complied with."[6]

[2] Common Criteria based European Cybersecurity Certification Scheme
[3] EU 5G Cybersecurity Certification Scheme
[4] EU Cybersecurity Certification Scheme for Cloud Services
[5] For example the Medical Devices Regulation ((EU) 2017/745) & the Machinery Regulation proposal (COM(2021) 202)
[6] Please refer to the supplementary expert opinion on the compatibility between the CSA and the NLF by Prof Gerald Spindler, page 32.

About us

The TÜV Association represents the policy and technical interests of its members, the TÜV organisations, which provide conformity assessment and technical services in almost all sectors of industry and commerce. TÜV stands for neutral and independent conformity assessment, such as testing (e.g. of household appliances, food or medical devices), inspection (e.g. of steam boilers, power plants or lifts), certification (e.g. of management systems or consumer products) and validation/verification (e.g. of greenhouse gas emission projects and reports).

Contact person - EU cybersecurity legislation

Rainer Gronau, LL.M.Eur.

Director Division Politics, Law, Europe, HR
Email: rainer.gronau@tuev-verband.de
Tel. +49 30 760095 490
www.tuev-verband.de/en