February 2022

Prof Dr Gerald Spindler (University of Göttingen) on the

Compatibility of the Cybersecurity Act and the New Legislative Framework

Key statements of the supplementary expert opinion from the TÜV Association's perspective

As part of the EU Cybersecurity Strategy[1] from December 2020, the European Commission considered presenting a legislative proposal on connected products. This proposition was supported by the Council in its 'Conclusions on the cybersecurity of connected devices'. The Commission Work Programme 2022 now foresees a proposal for a Cyber Resilience Act.

Against this background, the TÜV Association commissioned a first expert opinion in 2020 to contribute to the policy debate on the future European cybersecurity legislation. The expert opinion analyses and evaluates four policy options. The expert comes to the conclusion that future legislation should link core elements of the New Legislative Framework (NLF) and the Cybersecurity Act (CSA) in a horizontal Union legal act in such a way that the new act makes the CSA schemes mandatory for the sector-specific directives and regulations. In doing so, "the CSA assurance levels should be referenced or transferred one-to-one to a streamline horizontal regulation, that's to say also with the conformity assessment procedures provided for there but without being voluntary."

Supplementary expert opinion

In order to further develop and substantiate the proposed policy option, the author was asked to detail the effects of the legislative act described under "Option B" of the expert opinion on different product groups and applications using concrete examples. In particular, the existing legislation (CSA and NLF – and here, the Radio Equipment Directive[2] and Machinery Directive[3]) should also be taken into account. Further details should be provided of the basic structure and orientation of the horizontal act already described in the expert opinion to enable a better assessment of its effects based on the scenarios presented. In addition, the matter of the regulatory efficiency of such new legislation should also be considered. Several products groups shall be used for developing the corresponding scenarios (consumer IoT devices, machinery products, cloud services).

[2] See 2014/53/EU
[3] See 2006/42/EC

Key statements of the supplementary expert opinion from the TÜV Association's perspective:

Status Quo of selected EU cybersecurity requirements

- "Overall, the TSD [**Toy Safety Directive**] [4] contains hardly any opportunities for taking cyber risks into account (...). The TSD – and Article 10(2) in particular – therefore does not provide any legal protection against unauthorised access (...)" (page 11)
- "The GPSR [**General Product Safety Regulation proposal**] proposal additionally lacks an all-embracing risk-based approach that would include products as well as services and processes, thus allowing for the holistic risk assessment envisaged in the CSA. Thus, even if the GPSR proposal establishes cybersecurity requirements for the products it covers, it fails to establish legislation that makes the CSA or horizontal cybersecurity legislation redundant." (page 6)
- "This definition [*note: "safe product", Article 3(2) GPSR proposal*] does not ensure risk-adequate protection against unauthorised access to the product by third parties (cybersecurity). Hence even the "new" definition of what constitutes a safe product fails to close the regulatory gap that has existed to date, missing an essential opportunity to set the course on the horizontal level." (page 5)
- "(...) the GPSR proposal does not provide for any risk-based approach and the inclusion of different conformity assessment procedures/modules (...)" (page 6)
- "Moreover, not all cybersecurity risks can be covered by the RED [R**adio Equipment Directive**] either, as it does not include software as a stand-alone product but rather only insofar as it is integrated into the product itself." (page 14)
- "The RED and downstream legislation based on this are thus unable to ensure a comprehensive legislatory approach to cybersecurity that would make a horizontal regulation redundant." (page 14)
- "Overall, it should be noted that the current MD [**Machinery Directive**] does not contain any explicit mention of cybersecurity risks. Given its systematic approach (especially in Annex I), this would actually have been expected. A link to the CSA is also lacking (...). In view of this shortcoming, a considerable need exists for legislative action to address cybersecurity and connectivity risks." (page 20)
- "The 'malicious attempts from third parties to create a hazardous situation' are specified here again explicitly, with reference to the hacker risk already mentioned. (...) A picture thus emerges overall of a regulation that takes cybersecurity risks into account and eliminates the shortcomings that currently still exist in the MD with regard to these risks." (page 22)
- "The MR proposal and the planned intertwining with the CSA can, for the most part, be agreed to. It covers machinery products themselves, but not the associated ICT services and processes." (page 22)

[4] See 2009/48/EC

- "With the adoption of an **EUCS candidate** scheme[5] in accordance with the CSA, the full range of cloud services would be considered in their entirety for the first time. In this respect, the EUCS candidate scheme represents a significant step in the direction of horizontal coverage of the security of cloud services. This goes far beyond the aforementioned European requirements such as those detailed in the DSA proposal, and would also lend substance to the as yet rather abstract requirements stipulated in Article 32 GDPR. However, according to the CSA, the schemes still only apply on a voluntary basis – as already highlighted in the first expert opinion." (page 29)
- "More promising in terms of binding application of the security requirements by the CSA in conjunction with the EUCS candidate scheme would therefore be horizontal regulation to ensure the necessary security. A legally binding reference to the security requirements for manufacturers and operators pursuant to the CSA and the EUCS candidate scheme could help to enhance the security of ICT services (in this case, cloud services) across the board – not least by classifying them according to the respective risks (...)." (page 29)

Need for new legislation

- "The legislation proposed to date does not comprehensively consider cybersecurity risks as envisaged by the CSA *per se*." (page 30)
- "To summarise, none of the legislative proposals or existing legislation to date position the CSA at the forefront of cybersecurity legislation for these areas or make it and its instruments mandatory." (page 31)

Key elements of a horizontal cybersecurity regulation

- "(...) a horizontal regulation on cybersecurity for products should involve a lean horizontal approach that refers to the CSA and applies to all products affected by the NLF and, in particular, also to sector-specific harmonised products (whether in a directive or regulation) as well as to services and processes as covered by the CSA." (page 5)
- "In a horizontal regulation encompassing products and services or processes with binding references to the CSA, the definition of a product would first need to be broadened to cover all product areas, regardless of whether they are subject to a harmonised sector-specific product-related directive or regulation." (page 6)
- "The security requirements would thus need to be extended to include protection against any foreseeable accidental or malicious impairment of the protection objectives (...). Following the holistic approach of the CSA, such horizontal cybersecurity legislation would also need to be extended to include services and processes taking due account of the risk-based approach of the CSA." (page 7)

[5] European Cybersecurity Certification Scheme for Cloud Services

Proposals to subject, scope, definitions and essential safety requirements

- "(...) the introduction of a lean singular horizontal regulation for the field of cybersecurity setting out basic mandatory cybersecurity requirements that apply to all products covered by the New Legislative Framework (NLF) irrespective of the sector but otherwise refer entirely to the Cybersecurity Act (CSA) and its schemes with regard to the requirements and conformity assessment procedures would be advisable. The cybersecurity requirements should be specified through the application of mandatory schemes in accordance with the CSA. The schemes thus referred to could then be made entirely mandatory, insofar as suitable CSA schemes exist. Conflicts between the CSA and its schemes and the horizontal cybersecurity regulation with harmonised standards could thus be avoided." (page 31f)

- "In order to prevent diverging cybersecurity requirements from arising from different requirements due to sector-specific directives and regulations or the CSA and the schemes based thereupon, the new horizontal regulation should include a general conflict-of-law rule to the effect that the safety requirements of the CSA and its schemes take precedence if they stipulate more stringent requirements than the sector-specific harmonised legislation." (page 32)

- "In order to take the parallelism and intertwining of NLF acts and the CSA into account and to cater to the requirement of a fast and efficient transition to mandatory conformity assessment procedures as well as the "better regulation approach", the CSA assurance levels should be referenced or transferred one-to-one to lean horizontal regulation, that is to say also with the conformity assessment procedures provided for therein but without being voluntary." (page 32)

- "As such, the security requirements would need to be extended to include protection against any foreseeable accidental or malicious impairment of the protection objectives, along the lines of the MR proposal. Furthermore, in accordance with the holistic approach of the CSA, such a horizontal cybersecurity regulation must also include services and processes, in the form of the risk-based approach of the CSA." (page 32)

- "The following fundamental (cybersecurity) requirement must form the core of any new horizontal cybersecurity regulation:

  '*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.*' (page 32)

- „This proposal would eliminate the main disadvantage of the CSA, namely its voluntary nature, and at the same time preserve the main advantages of the CSA, namely its holistic and risk-based approach." (page 33)

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