TÜV VERBAND

Prof. Dr. Gerald Spindler (University of Göttingen) on the

Compatibility of the Cybersecurity Act and the New Legislative Framework

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

As part of the EU Cybersecurity Strategy[1], the European Commission considers to present a legislative proposal for horizontal rules to improve the cybersecurity of all connected products in the second half of 2021. This proposition was supported by the Council in its 'Conclusions on the cybersecurity of connected devices' of 2 December 2020. Against this background, the TÜV-Association has commissioned an expert opinion to contribute to the policy debate on the future European cybersecurity legislation.

The expert opinion analyses and responds to the following questions:

1. What advantages does the CSA offer and which goals can it be used to achieve?
2. How can the CSA be classified legally vis-à-vis the European product legislation (NLF)?
3. Do regulatory gaps still exist or does any need exist for regulatory action with regard to the cybersecurity of products manufactured in accordance with the European harmonisation legislation?
4. Is the voluntary nature of the CSA with regard to proof of compliance with cybersecurity requirements compatible with European product legislation, which in principle assumes mandatory security requirements for products?
5. How can the New Legislative Framework (NLF) and the Cybersecurity Act (CSA) be linked?
6. Is there a need for further legal action on the European level to integrate cybersecurity requirements directly into the sector-specific directives and regulations (for machinery, toys, lifts)?

[1] See European Commission, JOIN(2020) 18 final.

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

Coherence between NLF and CSA

- "The Cybersecurity Act (CSA) offers a broad approach to the coverage of cybersecurity risks for the first time. It not only applies to products like the sector-specific product safety directives or regulations do, but also covers services and processes – and thus enables a holistic approach." (p. 12)
- "To date, cybersecurity requirements have not been included in the sector-specific directives or regulations such as the Machinery Directive at all – as far as can be seen, with the sole exception of the Medical Device Regulation […]." (p. 12)
- "The lack of mandatory European cybersecurity requirements is particularly critical given that cybersecurity is now recognised as playing an important, if not central, role in products and plants that are increasingly dependent on IT environments." (p. 12)
- "The CSA can be classified legally as a horizontal regulation that deals comprehensively with cyber threats." (page 15)
- "The CSA includes key structural elements of the NLF, namely a risk-based approach, a link between the conformity assessment procedure to be applied and the risk posed by the product, the instrument of accreditation, the presumption of conformity, and the use of norms and standards. It is thus fully compatible with the NLF." (p. 15)

Regulatory gaps in the context of the product safety definition

- "This definition *(note: the product safety definition according to the General Product Safety Directive 2001/95/EC)* does not yet include the requirement that a product must also offer a risk-adequate protection against cyber attacks and misuse (protection of the integrity, confidentiality and availability of the systems) in order to guarantee the high level of protection enshrined in European product safety law. This regulatory gap is all the more serious because the product's interaction with IT services or processes within an IT environment is not taken into account either." (p. 16)
- "Such a regulatory gap also exists in the sector-specific product safety directives." (p. 16)
- "The CSA attempts to fill this regulatory gap in the area of cybersecurity with a holistic approach, whereby products are not considered in isolation, but rather the associated IT services and processes and thus also the mutual dependencies of products with these services and processes are also taken into account in the security consideration." (p. 17)

Voluntary nature of the cybersecurity requirements

- "However, the CSA lacks the element of mandatory conformity assessment, as certification has only been envisaged as voluntary so far – even for high risks or assurance levels. This CSA concept, which is initially based on voluntary conformity assessment procedures, thus contradicts most of the mandatory requirements provided for in the sector-specific harmonisation legislation and the associated conformity assessment procedures." (p. 17)
- "As long as the CSA still lacks mandatory schemes because there are no Union legal acts declaring the schemes mandatory, and harmonisation legislation does not (yet) contain any requirements regarding cybersecurity either, **a considerable need for regulation** still exists." (p. 17)
- "At the very least, however, it can be deduced from Article 169 TFEU that in the case of known risks, such as cybersecurity risks, an approach such as the one currently pursued by the CSA, namely based exclusively on voluntary cybersecurity requirements and a voluntary conformity assessment, cannot suffice. […] A purely voluntary compliance with cybersecurity requirements is hardly suitable for achieving a high level of consumer protection. In view of other mandatory product safety requirements, it is all the more difficult to understand why the increasingly important cybersecurity requirements should be treated differently to safety requirements. Especially since the control of products via ICT processes and their interconnection in corresponding IT environments has a considerable impact on their security." (p. 18)
- "An urgent need for regulation exists with regard to the necessary creation of a high level of consumer protection and the guarantee of the protection of high-ranking legal interests. This relates to the voluntary nature of cybersecurity requirements and the associated conformity assessment procedures provided for in the CSA to date. These must be interlinked with the GPSD and the sector-specific harmonisation legislation, for example by making the schemes mandatory for the respective area of application." (p. 19)
- "As previously mentioned, however, the voluntary nature of compliance with cybersecurity requirements and also certification cannot be reconciled with the mandatory procedures and compliance with product safety requirements provided for in the NLF decision. […] The outcome is fundamental differences in the level of safety and security regulation here." (p. 19)

Options for the integration of mandatory cybersecurity requirements

- "The question therefore arises of the integration of cybersecurity requirements into the NLF or corresponding product safety directives in order to make these mandatory. Several options are possible within this framework, which are to be assessed in light of the need for the speediest and most efficient possible transition from voluntary to mandatory certification procedures called for in Article 56(3) e) CSA." (p. 21)

Option A: Horizontal regulation within the framework of the NLF with elements of the NLF (p. 21 ff.)

- „Such a horizontal regulation could not meet the complex requirements of the different products and services in a uniform manner, however, especially with regard to their interaction with IT services and processes." (p. 22)
- "Furthermore, the fact that the CSA already provides for instruments that can be used that would also be in line with the EU's "better regulation" approach speaks against a horizontal product safety regulation that takes IT security risks into account." (p. 23)
- "Finally, the notion of the efficient use of resources also speaks against a new horizontal cybersecurity regulation, since the creation of a comprehensive procedure for the development of schemes by the Commission, ENISA and participating stakeholders with the CSA would already provide the corresponding structures." (p. 23)
- "To summarise the above arguments, such a new horizontal cybersecurity regulation would lead to contradictions, distortions and unnecessary duplications compared to the CSA. This approach should therefore be rejected." (p. 23)

Option B: Horizontal regulation with reference to the CSA (p. 24)

- "A [...] solution would be 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 NLF, irrespective of the sector, but otherwise referring entirely to the CSA and its schemes with regard to the requirements and conformity assessment procedures." (p. 24)
- "Specification of the cybersecurity requirements should take place through the application of mandatory schemes based on the CSA." (p. 24)
- "In order to take the parallelism and interlinking of NLF acts and the CSA into account and to meet 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 a streamline horizontal regulation, that's to say also with the conformity assessment procedures provided for there but without being voluntary." (p. 24)

Option C: Adaptation of the sector-specific harmonisation legislation with reference to the CSA (p. 24 f.)

- "A [...] similar solution would be to refer to the CSA schemes, including the risk levels, in the respective product-specific directives and regulations. Similar to the horizontal regulation approach discussed above, this would also ensure that the schemes become mandatory beyond the CSA, whereby the assessment procedures adapted to the respective risk levels would be included, [...] ." (p. 24 f.)
- "This *(note: a corresponding reference clause)* could also be a dynamic reference, for example, whereby only products that at the same time fulfil the conditions laid out in the CSA and the

schemes relevant to them are considered secure." (p. 25)

Option D: Adjustment of the sector-specific harmonisation legislation with no reference to the CSA (p. 25)

- "A [...] sector- or product-specific solution could include cybersecurity requirements in the respective NLF directives or regulations." (p. 25)
- "The same objections apply here as for the first proposal, namely those of the duplication of requirements and potential clashes between the sets of provisions." (p. 25)

Conclusion

- "A review of the possibilities to link the NLF and the CSA reveals that the second solution mentioned above *(note: Option B)* should be pursued. This approach would make the CSA schemes mandatory for the sector-specific directives and regulations through a horizontal Union legal act – most likely a regulation." (p. 25)
- "The corresponding conformity assessment procedures or risk levels of "basic", "substantial" and "high" should then also be adopted. Only such a procedure would allow unnecessary duplication and possible inconsistencies between the product safety legislation and the CSA to be avoided." (p. 25 f.)