Proposal for a realistic way to implement a "Cybersecurity regulation in Europe"

Prof. Dr. Dieter Wegener
DKE Vicepresident
Chair of DIN Presidential Committee FOCUS.ICT

02.02.2021
Industry view:

Cybersecurity is a MUST!
NLF and CSA - Two parallel approaches for regulation
EU-wide Cybersecurity Requirements

Executive Summary

With the following proposal, German industry is making an important contribution to the implementation of the new EU cyber security strategy to make Europe’s future digital, resilient, and secure. German companies strive to offer fail-safe cyber-resilient products, processes, and services. To this end, it is important that their efforts to strengthen cyber resilience are supported by consistent and EU-wide uniform requirements. As more than one regulation is often applicable to products, consistent and coherent requirements are essential for maintaining international competitiveness.

Industry proposal for consistent cybersecurity requirements for Europe

German Industry expressively supports the European Commissioner’s current considerations, supported by the European Council, to introduce mandatory, horizontal cybersecurity requirements based on the principles of the New Legislative Framework (NLF). When introducing a respective legislative proposal, the following recommendations should be considered:

1. To achieve overarching cyber resilience, generally binding protection targets should be defined by law and these should then be specified by harmonised European standards (ENs), that reflect the dynamic development of the state of the art.

2. Protective measures and resilience against cyber-attacks must be based on specific application and the associated threat situation. The NLF allows the assessment of different risk levels and follows the necessary risk-based approach. In this context, it is the responsibility of the manufacturer as the economic actor placing the product on the market to determine the intended area of use (and thus the threat level) of the product.

3. CE marking, by combining conformity assessment and market surveillance, acts as an anchor for trust for private and commercial customers alike.

4. The Digital Single Market will only be successful if national isolated solutions are avoided and compatibility with international standards is ensured.

5. With a bridge between the cybersecurity requirements of a product-centric horizontal NLF-based EU legislative act and the standards under the EU Cybersecurity Act (CSA), the two approaches can complement each other. Thus, coherent cybersecurity requirements can be guaranteed for the products falling into the scope of the two legislative acts.

6. Coherent cybersecurity requirements allow the manufacturer to choose between harmonised European standards (ENs) and CSA schemes to perform the conformity assessment according to NLF-based EU legislation. If a NLF is applied, the manufacturer can use the presumption of conformity.

(issued 2. February 2021)
NLF-CSA-Bridge
based on: CSA art. 54, par. 3

CSA voluntary certification

NLF obligatory for products covered conformity assessment

CA Moduls
Decision EU No. 768/2008

Scheme XOR* Standard

Standards hEN, EN, ISO/IEC
Standards IETF, W3C, ...
(includes design/test requirements)

application of hEN (obligatory): Presumption of Conformity

*XOR-Logic Freedom of choice for the manufacturer (only one - not twice):
The application of a CSA scheme as part of a conformity assessment procedure leads to compliance with the NLF legal act.
Implementation Strategy

2023 → Horizontal cybersecurity regulation adopted

2027/28 → NLF regulation-requirements mandatory after transition period (realistically 4 to 5 years)
    → Harmonized standards available
    → Presumption of conformity
Industry view:
NLF Transition Period needs realistically from 4 to 5 years

1 creation of WGs, drafting and approval of standards

2 preparation starts with stable/final standard, execution of measures with EU OJ listing
Implementation Strategy

2023 → Horizontal cybersecurity regulation adopted

2027/28 → NLF regulation-requirements mandatory after **transition period** (realistically 4 to 5 years)
→ Harmonized standards available
→ Presumption of conformity

**parallel**

2021 → RED delegated act including cybersecurity standardization request should be so open, that the RED cybersecurity approach will be reusable in the horizontal cybersecurity regulation