Statement on the Proposal for Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)

March 2021

DIN e.V.

Saatwinkler Damm 42/43
13627 Berlin
Germany
www.din.de

Contact:

Katja Krüger
Senior Government Relations Manager
Phone: 030 2601-2439
Fax: 030 2601-42439
Mail: katja.krueger@din.de

DIN, the German national standardization body, welcomes and supports the proposal for an update of the directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) that seeks to improve resilience and incident response capacities of public and private entities as well as competent authorities. We see the imperative need for a harmonized and future-proof European cybersecurity framework and in this regard expressly refer to our joint BDI-DIN-DKE position paper "EU-wide Cybersecurity Requirements Introduction of horizontal cybersecurity requirements based on the New Legislative Framework and bridge to the EU Cybersecurity Act". Common and harmonized cybersecurity requirements are the most efficient way to achieve a higher level of cyber resilience.

Anticipating this note, we have the following comments on the present draft:

Recital 28 (p. 18):

The recital contains a number error. Instead of ISO/IEC 29**41**7, it should read "In this regard, international standards ISO/IEC 30111 and ISO/IEC 29**14**7 provide guidance on vulnerability disclosure respectively". ISO/IEC 29147 covers "Information technology — Security techniques — Vulnerability disclosure".

Article 4 "Definitions" (p. 31-34):

Harmonized definitions are necessary to ensure consistent and uniform implementation of legislation. We therefore suggest to align the definitions in NIS2, such as data center or cloud computing, with international standards.

Article 6 "Coordinated vulnerability disclosure and a European vulnerability registry" (p. 35f):

We recommend the alignment of coordinated vulnerability disclosure with international standards such as ISO/IEC 29147 and ISO/IEC 30111.

Article 12 "Cooperation Group", paragraph 4b (p. 40):

The paragraph assigns the Cooperation Group with the task to exchange best practices and information on standards and technical specifications in relation to the implementation of the Directive. The multi-stakeholder platform on ICT standardization that was established by the European Commission to advise the Commission on matters related to ICT standardization policy, priorities, work programme and standardization needs in support of European legislation and policy, can be an important and helpful partner in this. In collaboration with the Commission, the platform drafts the annual Rolling Plan on ICT Standardization, that lists EU policy priorities where standardisation plays a key role in the implementation of the policy and also covers technologies of horizontal importance. We therefore highly recommend that the Cooperation Group cooperates with the multi-stakeholder platform and the European Standardization Organizations CEN, CENELEC and ETSI on identifying existing standards with relevance for the implementation of the Directive and further standardization priorities.

Article 18 "Cybersecurity risk management measures", paragraph 5 (p. 45f.):

A reference should be inserted here that the Commission can initiate standardisation projects according to Regulation 1025/2012 where no corresponding standards exist yet. The following text proposal should be added to the end of the paragraph:

> "Where no suitable European or international standards exist, the Commission shall use the possibility of issuing standardisation requests to the European Standards Organizations according to Regulation 1025/2012 to initiate the development of standards in order to substantiate the elements referred to in paragraph 2".

Article 21 "Use of European cybersecurity certification schemes" (p. 48f.):

We disapprove of the sole focus on specific European cybersecurity certification schemes in order to demonstrate compliance. Rather, we urge the European Commission to propose a legislative act containing horizontal cybersecurity requirements based on the New Legislative Framework (NLF) as layed out in our joint BDI-DIN-DKE position paper "EU-wide Cybersecurity Requirements Introduction of horizontal cybersecurity requirements based on the New Legislative Framework and bridge to the EU Cybersecurity Act". This approach is currently discussed in the European Commission (DG GROW and DG CNCT) and supported by the European Council's Conclusions on cybersecurity of connected devices as approved on December 2, 2020[1]. With a bridge between the cybersecurity requirements of a product-centered horizontal NLF-based EU legislative act and the schemes under the Cybersecurity Act (CSA), the two approaches can complement each other and coherent cybersecurity requirements can be guaranteed.

Article 22 "Standardization" (p. 49):

We expressly welcome the fact that priority is given to European and international standards.

[1] Council Conclusion on the cybersecurity of connected devices from December 2nd, 2020: "The Council of the European Union, […] STRESSES that cybersecurity requirements should be defined in line with the relevant Union legislation, including the CSA, the NLF, the Regulation on European Standardisation and a possible future horizontal legislation, to avoid ambiguity and fragmentation in legislation." (p. 4)