POSITION | CYBERSECURITY | EU LEGISLATION

EU-wide Cybersecurity Requirements

Introduction of horizontal cybersecurity requirements based on the New Legislative Framework and bridge to the EU Cybersecurity Act.

February 1, 2021

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 risk-adequate 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 expressly supports the European Commission'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 (hEN),*** that reflect the dynamic development of the state of the art.
2) Protective measures and resilience against cyber-attacks must be based on the specific application and the associated threat situation. The NLF allows the ***coverage 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 of 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-centred horizontal NLF-based EU legislative act*** and the ***schemes*** 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 (hEN) and CSA schemes*** to perform the conformity assessment according to NLF-based EU legislation. If a hEN is applied, the manufacturer can use the presumption of conformity.

BDI Bundesverband der Deutschen Industrie e.V.
DIN
DKE

Table of contents

Need for mandatory horizontal cybersecurity requirements

The increasing spread of digital technologies is creating a wide range of new opportunities – for both private and commercial users. At the same time, digitalisation also poses numerous challenges in terms of safety and security as well as privacy, which can lead to additional risks. These risks can be mitigated by employing targeted technical, regulatory, and behavioural measures (such as security-by-design). The remaining residual risks can be reduced accordingly by applying the state of the art of measures to strengthen resilience.

A high degree of cyber resilience is a basic prerequisite for the trouble-free functioning of highly digitalised processes, connected products and services. Coherent legal provisions are the key to maintaining the international competitiveness of German and European industry. It is important to consider that products – understood as hardware, software and combinations thereof – are integrated into highly complex systems, which means that, when regulating, these interactions must also be accommodated. Hasty additions and extensions to legal requirements concerning the cyber resilience of products must be avoided. In this context, BDI, DIN and DKE expressly welcome the European Council's conclusions on the cybersecurity of connected devices from December 2, 2020, in which the Council underlines the need for complementary and comparable requirements for cybersecurity functionalities of IT systems and IT components.

At the same time, requirements which aim at increasing the resilience against cyberattacks must be continually adapted to changing threat scenarios and intensities. Rigid legal requirements alone cannot accomplish this. Rather, laws and harmonised European technical standards (hEN) must go together to meet the dynamic requirements for enhanced cyber resilience.

Introduce horizontally mandatory cybersecurity requirements in accordance with the principles of the New Legislative Framework

There are currently several plans to include cybersecurity requirements in various product group-specific directives, such as respective considerations concerning the Machinery Directive (2006/42/EC) and delegated acts of the Radio Equipment Directive (RED) currently under preparation. German industry supports the approach taken by the European Commission to introduce a horizontal mandatory cybersecurity legislative act based on the principles of the New Legislative Framework (NLF). In this regard, BDI, DIN and DKE expressly welcome the European Council's fundamental support for this project.[1] We also fully support the intention to present the draft of a respective Single Market act under the NLF by the fourth quarter of 2021 at the latest. Such a horizontal approach is preferable to introducing cybersecurity requirements in different product-specific legal acts, as it avoids fragmentation of cybersecurity requirements. However, contrary to point 12 of the Council Conclusions, the primary goal of the coming months should be the development of mandatory, horizontal cybersecurity requirements based on the principles of the NLF. The development of voluntary schemes for connected products and services based on the EU Cybersecurity Act (CSA) should be avoided, since in future, the horizontal NLF-based cybersecurity requirements will serve this purpose.

From the perspective of German industry, the following six factors speak in favour of a horizontal NLF-based approach on cyber security:

[1] Cf the European Council's conclusions of December 2, 2020, on cybersecurity of networkable IT products (13629/20).

1) Define protection targets by law, regulating details in harmonised European Standards

While compliance with the requirements stipulated in the schemes of the CSA is a priori voluntary, mandatory requirements for products are only possible via an NLF-based legislative act (pursuant to Decision 768/2008). In general, horizontal requirements are preferable over integrating cybersecurity requirements into vertical, product group-specific acts, as a horizontal approach avoids fragmentation of cybersecurity requirements and at the same time, ensures coherence of requirements.

The strength of the NLF lies in the interaction between legislative requirements and harmonised European Standards (hEN). These standards are developed by European standards organisations based on a standardisation mandate from the Commission to specify the details of harmonisation legislation according to Regulation (EU) 1025/2012, and which, after an assessment by the EU Commission, are listed in the EU Official Journal. The EU institutions set out the essential requirements for products in directives and regulations. Examples are the Electromagnetic Compatibility Directive, the Low Voltage Directive, and the Machinery Directive. The technical specifications are then defined in standardisation committees by experts, for example from the public sector, as well as from industry, research, consumer, health, environmental and occupational safety organisations. They develop technical standards that are harmonised throughout Europe. For developing these hEN, the European standards organisations CEN, CENELEC and ETSI serve as moderation platforms. Through the national mirror committees, the process is open to all interested stakeholders. The progress of standardisation is transparent to all, so that there is a high degree of predictability on all sides. Decisions are made by consensus, enjoy broad acceptance, and have relevance for the entire internal market. This division of labour frees the European legislator of the burden of drafting detailed regulations. Thereby, the legal framework is kept flexible, and the resulting standards are practical, and thus, easy for companies to implement. After an assessment of conformity by the manufacturer or by third parties, the products can be freely marketed throughout the Single Market. Here, the principle “one standard, one test, accepted everywhere” applies.

The interaction between harmonised European standards and legislative requirements means that the legislator can focus on the formulation of protection targets, and that the technical details for implementing these targets are specified through standardisation. Thereby, the further development of the state of the art is efficiently considered. Since the introduction of the New Approach in 1985 and its further development into the New Legislative Framework (EC Regulation 765/2008), this interaction has proven itself over the last 35 years and is also predestined for the new challenges of cyber security in the context of digitalisation. BDI, DIN and DKE are convinced that the NLF offers a suitable approach for creating a regulatory framework for connected products in the EU Single Market.

BDI, DIN and DKE are therefore in favour of defining horizontal essential requirements on cybersecurity based on the principles of the NLF. The concrete formulation of the legal requirements would take place via standards as described. For this purpose, recourse can be made to the respective standardisation bodies for the development of hENs in the field of cyber security in which the experts are active.

The Electromagnetic Compatibility Directive (EMC) can be cited as a best practice for the definition of horizontal, cross-product group requirements. It regulates electromagnetic compatibility horizontally as a phenomenon directive, regardless of where the phenomenon of electromagnetic compatibility is to be observed. As a so-called "catch-all directive", the EMC Directive thus covers all end products for which electromagnetic compatibility is important. Likewise, the horizontal cybersecurity requirements based on the NLF should regulate aspects of the phenomenon “cybersecurity” independently of product groups. Fulfilling these requirements shall be understood as a prerequisite for placing a product on

the internal market. For example, the horizontal cybersecurity requirements based on the NLF shall foresee the implementation of security-by-design, proper encryption, and secure passwords.

2) Innovation-friendly and technology-open approach: Applying the state of the art

Not only potential attack vectors, vulnerabilities and threat scenarios are constantly changing, but also protective measures are constantly developed by companies and cyber security researchers. Especially for cyber resilience requirements, the NLF's innovation-friendly and technology-open approach is predestined to develop practical requirements.

3) Covering different risk levels

However, protective measures and resilience to cyber-attacks must always be geared to the application and the associated threat situation. It would be neither technologically nor economically expedient if smart home solutions had to meet the same requirements as components that are of paramount importance for the integrity and availability of critical infrastructures (cf. critical components pursuant to Paragraph 2 (13) of the German IT Security Law 2.0). Therefore, a “one-size-fits-all” solution would be the wrong approach. Carrying out conformity assessments and CE marking in accordance with the requirements laid down in regulations under the NLF are established practice in most companies. In addition, they enable risk-based conformity assessment procedures (from manufacturer self-declaration to unit verification (module A to G)) and are thus suitable for a wide range of products and fields of application.

4) Obligations of economic operators

The Decision 768/2008/EC establishing the NLF provides general obligations for all economic operators along the entire supply chain – these are manufacturers, authorised representatives, importers, and distributors, including online trade operators. All economic operators must take the necessary measures to ensure that only products that comply with the applicable legislation enter the EU market. Manufacturers and importers must comply with the applicable requirements when offering products for sale or placing them on the market.

The protection target “cyber resilience” requires a holistic approach. The introduction of cybersecurity requirements in a legislative act in accordance with the principles of the NLF is directed at manufacturers, as those placing products on the market, and should be supplemented by complementary legislative requirements – outside the NLF – for corresponding operator obligations.

5) Placing on the market, CE marking and market surveillance

The NLF focuses on the placing of a product on the market, i.e. the initial provision of a product on the European Single Market. The aim is to ensure that all products and services placed by manufacturers and importers on the European Single Market meet the requirements for safety and security, to guarantee safe commissioning.

The CE marking is the conformity marking of the NLF approach. The NLF provides transparent conditions for conformity marking and declaration of conformity. The application of the CE marking has been tested and established for many years. Private and commercial users recognise the compliance with corresponding requirements by the CE marking. Thus, by combining conformity assessment and market surveillance, the CE marking acts as an anchor of confidence for private and commercial customers alike.

A central component of the NLF approach is market surveillance. In Germany, for example, this is carried out for both the Electromagnetic Compatibility and Radio Equipment Directives by the Federal Network Agency. Market surveillance ensures that only products that meet the relevant requirements are placed on the internal market with the CE marking. Consequently, the legislator must empower the competent authorities for market surveillance, also regarding the area of “cyber security”, to be able to competently carry out and/or commission tests to ensure compliance with the required protection targets. From the perspective of German industry, the role of the Federal Network Agency as a competent body for market monitoring can be regarded as best practice.

6) Avoid national isolated solutions, ensure international compatibility

Cybersecurity is a global challenge. Consequently, national go-it-alones are not expedient. The European Single Market is a successful model that must be continued – especially in the digital age. The Single Market is a model for other markets and sets standards for product requirements and conformity assessment procedures that allow rapid market access and are innovation friendly. For this reason, BDI, DIN and DKE are opposed to a regulatory fragmentation of the European Single Market and to national go-it-alones. Maintaining the cyber resilience of products, processes and systems requires European regulatory approaches that are globally compatible. Therefore, legislative requirements concerning the cyber-resilience of products should be based – as far as possible – on international uniform technical standards. This would be very much in the interests of German industry, which is strongly geared to globalised value creation.

Taking all advantages mentioned above into account, German industry urges policy-makers to quickly introduce horizontally binding cybersecurity requirements based on the NLF and have them come into force by no later than 2023, in order to achieve effects as soon as possible – while observing appropriate transition periods. The goal must be to define basic cyber resilience requirements for all products – in the scope yet to be determined – destined for the European Single Market. Only in this way, will Europe be able to exploit the potential of digitalisation in the long term and at the same time proactively manage the associated risks.

Bridge between horizontal NLF legal act and CSA schemes

Only content-wise coherent legal requirements ensure that economic actors can apply them to their products, processes, services, and systems. German industry is firmly in favour of introducing horizontally mandatory cybersecurity requirements based on the principles of the NLF. In contrast, the CSA is pursuing the development of EU-wide harmonised certification schemes for voluntary certification. Under certain conditions, the CSA also envisages the possibility of making certification mandatory under individual schemes, but this would conflict with the NLF Decision (768/2008). However, the CSA also envisages the possibility that schemes can be utilised under a legal act for the respective conformity assessment procedure. This provides a bridge between the horizontal cybersecurity legal act based on the NLF and the schemes developed under the CSA. Article 54(3) CSA (EU 2019/881) provides the legal basis for this:

"Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.“

Consequently, for product groups for which a voluntary cybersecurity certification scheme has already been developed based on the CSA, this scheme could be used optionally and alternatively to

demonstrate compliance with the horizontal cybersecurity requirements under a future NLF-based legislative act, provided there are no contradictions in the requirements. Accordingly, the use of a scheme as part of a conformity assessment process would lead to compliance with that NLF legislative act. However, in the event of a contradiction, the NLF act must prevail.

The more similar the content requirements of a scheme are to existing and future harmonised European standards, the easier it will be to implement this procedure. Therefore, we call on all responsible for the CSA process, to synchronise closely with the standardisation projects and to concentrate primarily on the "Europeanisation" of existing national schemes. Divergence of the requirements set out in a CSA scheme and those pursuant to a hEN recognised under the NLF must be avoided at all costs for the reasons outlined above. Rather, as emphasised in points 10 and 11 of the Council Conclusions of December 2, 2020, greater emphasis should be placed on the development of European and international norms and standards for the cybersecurity of connected products.

Cybersecurity requires a holistic approach involving all stakeholders

All actors must contribute their share to ensure a risk-adequate level of cybersecurity: this equally concerns manufacturers as well as private and commercial users. Since products intended for commercial and private use are connected, it would be insufficient if only some users and manufacturers were investing in cybersecurity. Consequently, success, i.e. a holistic strengthening of the cybersecurity level across Europe, can only be achieved if all act in concert and the measures are coordinated. In addition, a coordinated approach must be enabled by law and implemented in practice. Holistic cybersecurity strategies with efficient protective measures can reduce the risk of cybersecurity incidents and thereby holistically strengthen cyber resilience. The goal must be to close dangerous gaps and vulnerabilities by taking swift and appropriate action to prevent potential attackers from exploiting them. The holistic approach is more than the sum of the individual measures of each economic actor. Each actor must make its predefined contribution to a coordinated overall result.

In addition to industry, however, private users and government agencies are also required to contribute to strengthening and maintaining the cyber resilience of products and services. For example, the market surveillance implemented in the NLF obliges ***member states*** to equip their competent authorities for market surveillance in such a way that they can competently conduct and/or commission audits with regard to compliance with the required protection targets. This also applies the area of cybersecurity. German industry perceives the Federal Network Agency as a competent body for market surveillance as a best practice.

Imprint

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Editors
Dr Thomas Holtmann
Head of Department Environment, Technology, Sustainability
T: +49 30 2028-1550
T.Holtmann@bdi.eu

Dr Thomas Koenen
Head of Department, Digitalisation and Innovation
T: +49 30 2028-1415
T.Koenen@bdi.eu

Steven Heckler
Senior Policy Manager, Digitalisation and Innovation
T: +49 30 2028-1523
S.Heckler@bdi.eu

Johannes Benjamin Helfritz
DIN e.V.
Project Coordinator External Relations
T: +49 30 2601-2791
Benjamin.Helfritz@din.de

Johannes Koch
DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE
Head of National Standardisation Policy and Cooperation
T: +49 69 6308-268
Johannes.Koch@vde.com

Katja Krüger
DIN e.V.
Senior Government Relations Manager
T: +49 30 2601-2439
Katja.Krueger@din.de

BDI document number: D 1248