Prof. Dr. Gerald Spindler
Chair of Civil Law, Commercial and Business Law,
Multimedia and Telecommunications Law, Comparative Law
Institute for Business Law

University of Göttingen

Prof. Dr. Spindler, Platz der Göttinger Sieben 6, 37073 Göttingen

Platz der Göttinger Sieben 6
D-37073 Göttingen

Tel.: (0551) 39 - 27243
Fax: (0551) 39 - 24633
E-Mail: info@gerald-spindler.de

4 March 2021

Brief expert opinion

on the compatibility of the Cybersecurity Act and the New Legislative Framework

Prepared on behalf of VdTÜV e. V.

Index

I. Commissioning of an expert opinion

The client has asked the undersigned to respond to the following questions:

1. What advantages does the CSA offer and which goals can it be used to achieve? What added value does the CSA consequently provide compared to the current sector-specific directives and regulations (before the CSA came into force)?

2. How can the CSA be classified legally vis-à-vis the European product legislation (NLF)? Is the CSA consistent with the current product regulation and particularly the currently applicable risk-based approach and its tiered conformity assessment systems (from the manufacturer self-declaration to the independently monitored certification)?

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? Is legislative action needed to make the cybersecurity requirements set out in the CSA schemes (cf. Article 56(2) and (3)) mandatory without delay?

5. How can the New Legislative Framework (NLF) and the Cybersecurity Act (CSA) be linked? Which new legal acts or which adaptations to existing legislation would be necessary to link these?

6. How can fundamental cybersecurity requirements be integrated into European product legislation? 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)?

II. Fundamental principles

A. The Cybersecurity Act (EU (2019/881)) (CSA)

The Cybersecurity Act of the European Union (EU) essentially comprises “Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology

cybersecurity certification of and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)".[1] Unlike the EU's common product safety directives, the CSA is not a sector-specific product regulation, but rather a horizontal framework for the phenomenon of cybersecurity, which does not differentiate between products and services in its approach.

The CSA first and foremost contains specifications for a certification framework for cybersecurity. ICT products, services and processes are subject to the according certification through this regulation. Article 46(2) CSA describes the primary objective as follows:

> "(2) The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle."

In order to achieve this objective, ENISA shall prepare European cybersecurity certification schemes on behalf of the European Commission (Article 49 CSA), which shall essentially achieve the security objectives formulated in Article 51 CSA, in particular with regard to performing an analysis of cybersecurity vulnerabilities. A CSA scheme can be based on (harmonised) standards (Article 54(1) c) CSA):

> "c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;"

Furthermore, Article 54(2) CSA stipulates that the schemes must be consistent with any legal requirements that may apply, in particular those emanating from harmonised Union law.

ENISA has been tasked by the European Commission with concrete preparation of the schemes pursuant to Article 49(1) CSA in compliance with the procedural requirements laid out in Article 49(2)–(6) CSA. The Commission shall adopt implementing acts on this basis in accordance with

[1] Official Journal of the European Union, L 151, p. 15 ff. dated 07.06.2019, hereinafter referred to with the abbreviation "CSA".

Article 49(7) CSA in which the respective schemes for ICT products, services and processes shall be set out.

Pursuant to Article 52(1) CSA, three different assurance levels are to be specified within this framework, namely "basic", "substantial" and "high", which are commensurate with the respective risks in terms of the probability and impact of a security incident. Pursuant to Article 54(1) b) and d) CSA, the schemes must also contain descriptions of the risk associated with a product or service and the assurance level.

Pursuant to Article 53(1) CSA, manufacturers and suppliers can conduct a self-assessment for EU conformity for the "basic" assurance level. Pursuant to Article 53(2) CSA:

> "(2) The manufacturer or provider of ICT products, ICT services or ICT processes may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products, ICT services or ICT processes shall assume responsibility for the compliance of the ICT product, ICT service or ICT process with the requirements set out in that scheme."

Thus, the schemes must also contain information pursuant to Article 54(1) e) CSA on whether a self-declaration of conformity is permitted.

In addition, conformity assessment bodies in the sense of Article 60 CSA can also issue cybersecurity certificates for the "basic" assurance level (Article 56(4) CSA), as can public bodies (Article 56(5) CSA).

For the "substantial" assurance level or medium risk, Article 52(6) CSA requires a cybersecurity certificate, which can (according to Article 56(4) CSA) also be issued by conformity assessment bodies to be accredited pursuant to Article 60 CSA or by public bodies pursuant to Article 56(5) CSA.

Pursuant to Article 56(6) CSA, only national cybersecurity certification authorities or, in the event that tasks are delegated, conformity assessment bodies may issue certification for the "high" assurance level.

The interplay between the conformity assessment and certification is again emphasised in Recital 77, sentences 1–4 CSA:

> "A **conformity assessment** is a procedure for evaluating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled. That procedure is carried out by an **independent third party** that is not the manufacturer or

> provider of the ICT products, ICT services or ICT processes that are being assessed. A European cybersecurity certificate should be issued following the successful evaluation of an ICT product, ICT service or ICT process. A European cybersecurity certificate should be considered to be a confirmation that the evaluation has been properly carried out."

Additionally, Recital 81 CSA again makes clear:

> "The manufacturer or provider of ICT products, ICT services or ICT processes who carry out a conformity **self-assessment** should be able to issue and sign the EU statement of conformity as part of the conformity assessment procedure. An **EU statement of conformity** is a document that states that a specific ICT product, ICT service or ICT process complies with the requirements of the European cybersecurity certification scheme. By issuing and signing the EU statement of conformity, the manufacturer or provider of ICT products, ICT services or ICT processes assumes responsibility for the compliance of the ICT product, ICT service or ICT process with the legal requirements of the European cybersecurity certification scheme. A copy of the EU statement of conformity should be submitted to the national cybersecurity certification authority and to ENISA."

The main difference is thus that the EU declaration of conformity is issued by the manufacturer or supplier and they are responsible for its correctness, whereas in the case of certification, either the conformity assessment body or a public body issues the certificate.

However, for all of the risk levels mentioned above, certification (or, in the low risk range, the declaration of conformity based on self-assessment by the manufacturer) remains voluntary unless Union law or Member State law states otherwise. This is stipulated in Article 53(4) CSA on conformity self-assessment:

> "The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law."

For cybersecurity certification – and thus for the other risk ranges – in Article 56(2) CSA:

> "The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law."

In light of the respective cybersecurity aims, the Commission must reassess at regular intervals whether cybersecurity certification can remain voluntary or must be made mandatory (Article 56(3) CSA):

> "The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improve the functioning of the internal market."

Recital 92, sentence 1 CSA also makes clear that mandatory certification may be imposed in the future:

> "In some areas, it could be necessary in the future to impose specific cybersecurity requirements and make the certification thereof **mandatory** for certain ICT products, ICT services or ICT processes, in order to improve the level of cybersecurity in the Union."

Furthermore, Article 56(3) e) CSA requires the Commission to

> "propose the most speedy and efficient way in which the transition from a voluntary to mandatory certification schemes is to be implemented."

Article 54(1) c) CSA stipulates numerous other requirements for the schemes, in particular:

> "references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;"

Overall, however, Article 54(1) CSA grants the respective schemes extensive flexibility in the various elements required for cybersecurity certification, such as the maximum validity period for certification (Article 54(1) r) CSA).

Article 54(2) CSA stipulates the following in all cases:

> "(2) The specified requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements, in particular requirements emanating from harmonised Union law."

However, the legal implications of certification or an EU declaration of conformity are also important during the assessment, as they can demonstrate the presumption of conformity with the requirements of a specific legal act (Article 54(3), (4) CSA):

> "(3) 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.
>
> (4) In the absence of harmonised Union law, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements."

This presumption of conformity also applies to the certification. Thus, the presumption of conformity with the requirements of this respective scheme applies to certification according to Article 56(1) CSA.

> "(1) ICT products, ICT services and ICT processes that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme."

B. The New Legislative Framework

The New Legislative Framework (NLF) largely replaces the provisions set out in the New Approach in product safety. With "Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Council Regulation (EEC) No 339/93"[2], it provides a general horizontal framework for non-specified product safety regulations, whereby the regulation comes into effect alongside "Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products"[3]. Regulation 765/2008 has been replaced in part by the new "Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and the conformity of products, and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011"[4].

1. Market surveillance regulation (EU) 2019/1020

This regulation primarily foresees a fundamental reform of Directive 2001/95/EC on general product safety[5] (Recital 7). In particular, it aims to harmonise four areas across Europe (Article 1 Regulation No 765/2008):

[2] Official Journal of the European Union L 218, p. 30 ff. dated 13.08.2008.
[3] Official Journal of the European Union L 218, p. 82 ff. dated 13.08.2008.
[4] Official Journal of the European Union L 169, p. 1 ff. dated 25.06.2019.
[5] Official Journal of the European Union L 11, p. 4 ff. dated 15.01.2002.

- the accreditation bodies and corresponding procedure;
- market surveillance of products to ensure a high level of protection of health and safety in general, health and safety at the workplace, environmental and consumer protection, and security;
- the control of products from third countries;
- general principles for the CE marking.

Regulation 768/2008/EC has been amended and adapted in part by "Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and the conformity of products, and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011"[6].

However, pursuant to Article 2(1) Regulation No 2019/1020, this regulation only applies to products that are subject to the EU-wide harmonisation legislation listed in the annex.

Pursuant to Article 3(19) Regulation No 2019/1020, a "product presenting a risk" is understood to be

> "a product having the potential to affect adversely health and safety of persons in general, health and safety in the workplace, protection of consumers, the environment, public security and other public interests, protected by the applicable Union harmonisation legislation, to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the product concerned, including the duration of use and, where applicable, its putting into service, installation and maintenance requirements;"

Regulation No 765/2008 remains in force with regard to the provisions on conformity assessment bodies however – as is reflected in the amended title for Regulation No 765/2008 of "setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93" (Article 39(1) No 1 Regulation No 2019/1020.

[6] Official Journal of the European Union L 169, p. 1 ff. dated 25.06.2019.

2. Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008

Decision No 768/2008/EC provides for a more or less mandatory model for the design of sector-specific directives for all product safety directives. Particularly Article 4(1) b) of this decision provides for a risk-based approach for mandatory declarations of conformity:

> "(1) Where Community harmonisation legislation requires conformity assessment to be performed in respect of a particular product, the procedures which are to be used shall be chosen from among the modules set out and specified in Annex II, in accordance with the following criteria:
>
> (a) (...)
> (b) the nature of the risks entailed by the product and the extent to which conformity assessment corresponds to the type and degree of risk;"

Article 6(1) of Decision No 768/2008/EC again leaves it up to the (EU) Community which approach it wishes to take in the harmonisation legislation for conformity assessments and whether the assessment should be carried out by the manufacturer, a public authority or a notified body.

The risk categories correspond with the modules for declarations of conformity contained in the annex, beginning with Module A on internal production control through to Module H1 on conformity based on full quality assurance with design examination, which sets the most stringent requirements.

In the case of the declaration of conformity, Decision No 768/2008 also provides for a presumption of conformity (Article 3(2) in conjunction with Article R8).

> "Products which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in … [reference to the relevant part of the legislation]."

Recital 40 moreover states:

> "(40) If a conformity assessment body demonstrates conformity with the criteria laid down in harmonised standards, it should be presumed to comply with the corresponding requirements set out in the relevant sectoral legislation."

III. Question 1: Advantages of the Cybersecurity Act

1. What advantages does the CSA offer and which goals can it be used to achieve? What added value does the CSA consequently provide compared to the current sector-specific directives and regulations (before the CSA came into force)?

A. First horizontal framework

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.

The added value of the CSA compared to the current sector-specific directives and regulations for product safety thus primarily lies in the horizontal approach, which can identify IT risks across all areas. This facilitates the specification of requirements for both uniform cybersecurity measures and assessment procedures without differentiating between products and IT services (this differentiation is difficult anyway in practice). **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[7], which explicitly addresses the topic of IT security for the first time by qualifying software as an active device (Article 2(1) No 4) and requiring consideration of the interaction between software and the IT environment (Article 5 Para. 2 in conjunction with Annex I No 14.2 d)). The same applies to IT security measures, which are explicitly addressed in Annex I No 17.4 of the Medical Device Regulation. Apart from this exception, no comparable requirements exist to date in product-specific directives or regulations.

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. The CSA therefore offers a regulatory starting point for the development of cybersecurity requirements and establishes the according risk-appropriate review mechanisms.

B. Risk-based approach

The CSA offers a high degree of flexibility, whereby schemes can be developed specifically for classes of products and interacting services depending on the risk assessment by differentiating

[7] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, Official Journal of the European Union L 117, 1 ff. dated 05.05.2017

between “basic”, “substantial” and “high” risks. The CSA’s modular structure means that the schemes can be followed voluntarily or also declared mandatory through additional legal acts in Union law or by Member States. The link via Article 60 CSA to the common conformity assessment procedures and the NLF as well as the presumption of conformity of certification (Article 56 (1) CSA) or manufacturers’ self-declarations (for “basic” risks) (Article 54(3) CSA) mirrored in Article 3(2) Decision No 768/2008 in conjunction with Article R8 Decision No 768/2008 moreover ensures the creation of a single market, whereby the presumption of conformity means the respective Member States can trust that the cybersecurity requirements have been complied with.

However, the presumption of conformity pursuant to the CSA only applies if the assessment and certification procedure provided for in the respective scheme has been followed, which in turn depends on the assurance levels. If, for example, the products in question have been certified by third parties not meeting the requirements of Article 60 CSA, the presumption of conformity pursuant to Article 56(1) CSA cannot apply.

The parallels between the NLF (Article 4(1) b) Decision No 768/2008) and the CSA lie in the fact that an inseparable correlation exists in both the CSA and the NLF between the conformity assessment procedure to be applied and the risks posed by the product.

C. Summary

To summarise, the CSA offers the following added value:

- horizontal, uniform regulation of cybersecurity requirements
- inclusion of products as well as of ICT services and processes
- uniform requirements for assessment and certification procedures
- risk-based approach

IV. Question 2: Legal classification of the Cybersecurity Act

2. How can the CSA be classified legally vis-à-vis the European product legislation (NLF)? Is the CSA consistent with the current product regulation and particularly the currently applicable risk-based approach and its tiered conformity assessment systems (from the manufacturer self-declaration to the independently monitored certification)?

A. Cumulative application of the CSA and NLF

The CSA can essentially be classified legally as horizontal to the European product legislation in the form of the New Legislative Framework (NLF), whereby it applies in addition to the product safety requirements and complements the safety regulations with (still to be adopted) schemes.

Similar to in other safety regulations pursuant to public law, requirements pursuant to the CSA apply in addition to product safety regulations in a cumulative manner. In other words, the CSA is not replaced by sector-specific product safety directives, nor can the CSA claim precedence over these directives.

B. Risk-based approach

Both legal acts – the CSA and the NLF – take a risk-based approach. This is made clear in the CSA through the assurance levels mentioned previously, which link to the different risks and their intensity, and in the NLF through Article 4(1) b), which requires modules to be chosen according to

> "the nature of the risks entailed by the product and the extent to which conformity assessment corresponds to the type and degree of risk;"

Thus, the NLF's risk-based approach and the tiered conformity assessment systems provided for therein (from the self-declaration by the manufacturer through to an independent certification) do not contradict the approach taken in the CSA. As previously mentioned, the CSA provides for a self-declaration by the manufacturer as an EU statement of conformity for low risks (Article 53(2) CSA), but certification for higher risks (Article 56 CSA). The fact that the CSA also contains a risk-based approach is made clear in Recital 78 CSA:

> "The choice of the appropriate certification and associated security requirements by the users of European cybersecurity certificates should be based on an analysis of the risks associated with the use of the ICT products, ICT services or ICT processes. Accordingly, the assurance level should be commensurate with the level of the risk associated with the intended use of an ICT product, ICT service or ICT process."

Thus, the approach taken in the CSA corresponds to the risk-based approach provided for in the NLF.

The CSA is also aligned with the NLF with regard to the conformity assessment systems, and particularly the requirements set for the conformity assessment bodies, through the reference in Article 60(1) CSA to Regulation No 765/2008, whereby this regulation applies specifically for product safety and regulates aspects of accreditation, etc. and is, as such, not superseded by the new Regulation No 2019/1020.

C. Presumptions of conformity

The presumptions of conformity also apply in parallel: the CSA contains the presumption (Article 56(1) CSA) that the requirements of the CSA are complied with in case of certification,

including the manufacturer's self-declaration pursuant to Article 54(3), (4) CSA, and the NLF contains the presumption regarding compliance with product safety or the respective standards (Article 3(2) in conjunction with Article R8 Decision No 768/2008).

D. Mandatory assessments

A significant difference exists, however, with regard to the question of whether conformity assessments and certifications are mandatory: while the NLF provides for this in the modules (depending on the risk) – as is reflected in the Medical Device Regulation, again depending on the products' risk classification (Article 52 Medical Device Regulation) – the CSA does not stipulate a certification process – even for the "high" assurance level (Article 56(2) CSA), although the option of committing to certain safety requirements or applying certain conformity assessment procedures is already provided for therein.

E. Summary

The CSA can be classified legally as a horizontal regulation that deals comprehensively with cyber threats. It is based on broadly similar approaches to the sector-specific product safety directives, but takes a holistic approach as a horizontal regulation. Both legal acts are risk-based and contain presumptions of conformity, but differ considerably in terms of the obligation to apply the certification or conformity assessment procedure.

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.

V. Question 3: Regulatory gaps and need for regulatory action

3. Do regulatory gaps still exist or does any need exist for regulatory action with regard to cybersecurity for products manufactured in accordance with the European harmonisation legislation?

From Question 4: Is legislative action needed to make the cybersecurity requirements set out in the CSA schemes (cf. Article 56(2) and (3)) mandatory without delay?

A. Lacking obligation for certification / conformity assessment

The need for legal policy action with regard to the risk situation in the field of cybersecurity, especially in terms of the risks arising from Internet of Things devices, must form the starting point for answering this question.

While the General Product Safety Directive (GPSD) 2001/95/EC applies to consumer products, other sector-specific legislation also applies to these, too. With the exception of the Medical Device Regulation 2017/745, neither the GPSD nor the sector-specific legislation address specific cybersecurity risks however. Article 3(1) GPSD requires that manufacturers only place safe products on the market. According to Article 2 b), however, every product is considered a "safe product", which

> "[...] under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular:
> (i) the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance;
> (ii) the effect on other products, where it is reasonably foreseeable that it will be used with other products;"

This definition 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.

Such a regulatory gap also exists in the sector-specific product safety directives. Only the Medical Device Regulation[8] explicitly takes the interactions between software and its IT environment into account (Annex I No 14.2. d)

> "the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts;"

Annex I No 17.4. moreover states:

[8] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, Official Journal of the European Union L 117, p. 1 ff. dated 05.05.2017.

> "Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended."

However, these regulations on the consideration of cybersecurity risks are a clear exception in the sector-specific harmonisation legislation.[9] The pending revision of the Radio Equipment Directive[10] for which the EU has submitted an impact assessment report with options for integrating cybersecurity requirements should also be mentioned in this context.[11] Nor does the NLF contain a general provision that would make it mandatory to take cybersecurity into account in the risk assessment and selection of the respective modules with regard to certification and the manufacturer's self-declaration.

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. 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.

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. However, this does not prejudge the legal framework in which these regulatory gaps would have to be filled; this will be addressed in Section VII.

The fact that the Union legislator is called upon to act here not least arises from Article 169 of the Treaty on the Functioning of the European Union (TFEU), which obliges the EU to ensure a

---

[9] Also see Technical Report ISO/TR 22100-4 "Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machine manufacturers for consideration of related IT-security (cyber security) aspects", prepared as part of ISO/TC 199 "Safety of machinery".

[10] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance, Official Journal of the European Union L 153, p. 62 ff. dated 22.05.2014.

[11] Centre for Strategy and Evaluation Services, Final Report – Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment (April 2020), retrieved from https://ec.europa.eu/docsroom/documents/40763 on 21.10.2020

high level of protection for consumers. Similarly, Article 38 of the EU Charter of Fundamental Rights calls for a high level of consumer protection.[12] The objective of consumer protection and thus product safety has long been recognised in the case law of the European Court of Justice (ECJ) as part of the important general interests.[13] Safety is expressis verbis part of consumer protection, whereby this is generally understood to mean product safety.[14] However, it is equally recognised that Article 169 TFEU leaves the Community institutions the prerogative to assess how they want to ensure the level of consumer protection.[15] 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. This particularly applies if the harmonisation legislation ensuring product safety is not interlinked with the CSA accordingly or the cybersecurity requirements pursuant to the CSA are at least mandatory for higher risk areas or assurance levels. 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.

If the cybersecurity requirements or their certification are to become mandatory, there must be corresponding requirements in Union legislation (or from Member States). Otherwise, they can only become mandatory (indirectly) through corresponding referencing in the GPSD and the (sector-specific) harmonisation legislation on the schemes pursuant to the CSA. As such, there is a need for legislative action with regard to the voluntary nature.

B. Lack of schemes

It is additionally important to rapidly develop the necessary schemes. The CSA itself only provides for a framework within which cybersecurity certifications or manufacturer self-declarations can be issued or carried out based on schemes that are still to be developed. As long as such schemes do not yet exist, no certifications and manufacturer self-declarations on cybersecurity can be issued based on the CSA. As the responsible EU authority, ENISA is

[12] Grabitz/Hilf/Nettesheim/Pfeiffer, 71. EL August 2020, AEUV Art. 169 Rn. 2.
[13] Fundamental CJEU, Rs. 120/78, Slg. 1979, 649 - Rewe/Bundesmonopolverwaltung für Branntwein - “Cassis de Dijon”, No. 8.
[14] E.g. Grabitz/Hilf/Nettesheim/Pfeiffer, 71. EL August 2020, AEUV Art. 169 Rn. 10.
[15] Micklitz/Reich, EuZW 1993, 593; Grabitz/Hilf/Nettesheim/Pfeiffer, 71. EL August 2020, AEUV Art. 169 Rn. 18.

currently driving the development of such schemes however.[16] The European Commission has tasked ENISA with development of the first schemes for the recognition of common criteria (EUCC) and the certification of cloud services (EUCS).[17] ENISA's work programme also provides for a scheme for the certification of "consumer IoT devices".

C. Summary

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.

VI. Question 4: Compatibility of the voluntary Cybersecurity Act with the product safety legislation

4. Is the voluntary nature of the CSA with regard to proof of compliance with cybersecurity requirements compatible with European product regulation, which in principle assumes mandatory security requirements for products?

Article 56(2) and (3) CSA in principle provides for voluntary cybersecurity certifications, whereby this certification can also be made mandatory within the schemes developed by ENISA as the lead agency or stipulated as mandatory by the EU or the Member States, with the consequence that, depending on their assurance level, manufacturers or service providers require certification or must at least issue a self-declaration (Article 53 (4) CSA).

The voluntary nature of Article 56 (2) and (3) CSA does not affect the mandatory certification or manufacturer's declaration procedures provided for in the harmonisation legislation, however, as the CSA is cumulative to the requirements stipulated in this legislation.

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. Although the presumptions of conformity provided for in the CSA, in particular that the requirements of the schemes are met, largely correspond to those in the harmonisation legislation, these presumptions only apply when a manufacturer or operator complies with the cybersecurity

[16] See also *Kipker*, Datenschutz und Datensicherheit (DuD) 2020, p. 390 ff.
[17] See also https://www.enisa.europa.eu/topics/standards/Public-Consultations on 21.10.2020

requirements voluntarily (unless the schemes have been declared mandatory). The outcome is fundamental differences in the level of safety and security regulation here.

VII. Questions 5 and 6: Linking of the Cybersecurity Act with product safety legislation

5. How can the New Legislative Framework (NLF) and the Cybersecurity Act (CSA) be linked? Which new legal acts or which adjustments to existing legislation would be necessary to link these?

6. How can fundamental cybersecurity requirements be integrated into European product regulation? 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, etc.)?

With regard to the need for regulation mentioned in Section IV, Article 56(3) CSA explicitly stipulates that

> "The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improve the functioning of the internal market. The first assessment shall take place by 31 December 2023; subsequent assessments shall take place at least every two years thereafter."

Article 56(3) e) CSA moreover requires the Commission to

> "propose the most speedy and efficient way in which the transition from a voluntary to mandatory certification schemes is to be implemented."

In principle, a mandatory declaration of schemes pursuant to the CSA would not require any special linkage with the harmonised legislation, as the legal acts are to be applied cumulatively. Where Union acts declare the schemes mandatory, manufacturers of IT products covered by the schemes must comply with the schemes' corresponding security requirements.

The question nonetheless arises (especially with regard to a harmonisation of requirements) of the interlinking between both legal texts – in particular to avoid duplications and contradictions between requirements in the product safety directives and regulations pursuant to the NLF on the one hand and those pursuant to the CSA or the corresponding schemes on the other. However, as

long as the sector-specific harmonisation legislation – with the exception of the Medical Device Regulation – does not provide the corresponding requirements, these questions do not arise.

The only relevant question might be how to deal with possible duplications of assessments and potentially conflicting security requirements between schemes pursuant to the CSA and product safety requirements within NLF directives or regulations, which would then contain such cybersecurity requirements. These could for example occur within the framework of the Medical Device Regulation, which – as previously mentioned – in principle already regulates cybersecurity requirements. Bearing in mind that both sets of regulatory complexes are to be applied in parallel, certification would be required both pursuant to the Medical Device Regulation and a (currently hypothetical) scheme pursuant to the CSA. However, this argument is not really viable to rule out the interlinkage of the CSA and product safety directives or regulations. Existing certificates could on the one hand be taken into account within the certification pursuant to the Medical Devices Regulation – as is already mentioned in Article 54(3) CSA:

> "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."

On the other hand, the CSA itself provides for existing standards and safety requirements to be taken into account when developing corresponding schemes (Article 54(2) CSA); double tests could thus be avoided.

If one assumes, however, that the cybersecurity requirements pursuant to the CSA are to become mandatory in conjunction with a scheme, Union legislation is required pursuant to Article 53(4) CSA (or alternatively a Member State regulation, though this will not be examined in greater detail here, as the establishment of a single market should be ensured with harmonised 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.

A. Horizontal regulation within the framework of the NLF with elements of the NLF

Firstly, a horizontal regulation within the framework of the NLF, which sets uniform minimum requirements for the cybersecurity of all products and, depending on the risks, works with a self-declaration of conformity (manufacturer's self-declaration) or conformity assessments by

external conformity assessment bodies; the specific requirements would then be set out in harmonised standards. Such a horizontal regulation would be independent of the CSA.

The advantage of such a solution would be that minimum requirements, which are dependent on the adoption of schemes declared mandatory in the CSA, could be mandatorily set out here for IT products in the horizontal cybersecurity regulation.

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. While the setting of minimum requirements is conceivable, these would have to be tiered in a similar fashion to the CSA according to the respective risk factor that use of the products has or causes. Furthermore, the specific requirements for each product category, including the interdependencies with other IT services and processes, would have to be defined in extensive annexes in such a horizontal cybersecurity regulation.

This seems all the more inappropriate in light of the fact that the CSA itself in principle already provides for such a horizontal approach, but allows for a strong risk-appropriate differentiation precisely through the development of specific schemes (for products, processes, services, technologies). Consequently, an additional horizontal cybersecurity regulation would lead to inefficient duplications. Moreover, such a horizontal cybersecurity regulation would ultimately address the same risks as the CSA itself.

Uniform introduction of the manufacturer's self-declaration across the board could also only intervene in areas with low risks according to the NLF, namely Article 4(1) b) Decision 768/2008/EC in conjunction with Module A. Widespread introduction of the manufacturer's self-declaration on compliance with cybersecurity requirements would not be in line with the risk-based approach, which would also have to differentiate between the respective assurance levels within the framework of the NLF (analogous to the CSA). In other words, if self-declarations by the manufacturers were to be used widely as a conformity assessment procedure in such a horizontal regulation, it would practically be assumed from the outset that all cybersecurity requirements are only to be classified at the "basic" risk level (in the sense of Article 53 CSA). However, this would contradict the different assurance levels provided for in the CSA. It would be contradictory and lead to legal inconsistencies on the European level on the one hand to only presume a low risk on the product safety level with regard to IT risks making use of a manufacturer's self-declaration, while on the other hand to presume a differentiation according to assurance levels within the framework of cybersecurity certifications.

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[18] speaks against a horizontal product safety regulation that takes IT security risks into account:

> "Agree that legislation already in force should have been properly evaluated, to see whether existing tools could be used to do the job – before considering new initiatives;"

This regulatory objective clearly contradicts the creation of parallel structures or regulations pursuing the same objective, namely to create security for products associated with IT security risks.

Apart from this, it only remains to once again emphasise that the CSA goes beyond the NLF in that it not only concerns products, but also their interconnection with IT services and processes. Such a new horizontal cybersecurity regulation would therefore have to go beyond the framework set by the NLF to date and also extend to IT services and processes in general – as is the case in the Medical Device Regulation. Given the diversity of products, it seems doubtful whether a horizontal approach is possible for all products in the same way though.

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. It would also be questionable within this framework why referencing standards (yet to be created) in a possible new horizontal cybersecurity regulation should be preferable to adopting schemes, especially since Article 53(1) c) CSA provides for existing standards to be taken into account in the schemes:

> "references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;"

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.

---

[18] Better regulation for better results – An EU agenda, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 19.05.2015 COM (2015), 215 final, p. 9.

B. Horizontal regulation with reference to the CSA

A second 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. Specification of the cybersecurity requirements should take place through the application of mandatory schemes based on the CSA. The CSA schemes thus referred to could then be made mandatory across the board – depending on the existence of a CSA scheme. In other words, such a horizontal cybersecurity regulation would refer to the CSA schemes instead of harmonised standards; insofar as such schemes have been developed for specific products or services, they would become mandatory for all products covered by means of the "transfer effect" of the horizontal cybersecurity regulation, independently of sector-specific harmonised legislation. The clashes described between the CSA or its schemes and the horizontal cybersecurity regulation with harmonised standards (Section VII.A) could thus be avoided.

In order to avoid clashes between harmonised standards and subsequent schemes, only ENISA should be entrusted with the development of schemes in the event that no such schemes exist yet pursuant to the CSA. Otherwise, there would be a risk of diverging security requirements arising later, for example through harmonised standards that do not correspond to the schemes.

However, this does not answer the question of how compliance with the cybersecurity requirements set out in the schemes would be verified, and in particular whether the risk level and differentiation according to manufacturer self-declaration and cybersecurity certification requirements for the schemes would essentially be "incorporated in", with reference made to the CSA. 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. In other words, while no reference would be made to the voluntary nature, reference would be made to the material content of the schemes, including their linking with the corresponding envisaged assessment procedures depending on the respective assurance level.

C. Adaptation of the sector-specific harmonisation legislation with reference to the CSA

A third, 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, again from “basic” through “substantial” to “high”.

At first glance, the presumed disadvantage of such a reference clause aimed at the respective directives or regulations could be seen in the fact that each of the directives or regulations would have to be adapted accordingly and this could require additional efforts and lead to time delays.

However, the inclusion of a corresponding reference clause in the respective sector-specific harmonisation legislation would also be possible in an omnibus procedure in which similar or identical amendments referring to the CSA are added to several NLF directives and regulations in the course of a single legislative procedure. This 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.

D. Adjustment of the sector-specific harmonisation legislation with no reference to the CSA

A fourth sector- or product-specific solution could include cybersecurity requirements in the respective NLF directives or regulations. The necessary specification of cybersecurity requirements would then be developed through harmonised standards – autonomously and independently of schemes pursuant to the CSA. The applicable conformity assessment procedure to comply with cybersecurity requirements would also need to be evaluated or adjusted in the directives or regulations in each case. In particular, the manufacturer’s self-declaration provided for there until now would have to be re-evaluated with regard to products’ risk potential, which may have increased as a result of interconnection, and, if necessary, to prescribe the involvement of independent conformity assessment bodies.

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. There would be the added disadvantage just mentioned that each directive or regulation would have to be supplemented with the corresponding information and requirements. Reference can thus be made to the statements expressed in Section VII (A) above.

E. Conclusion

A review of the possibilities to link the NLF and the CSA reveals that the second solution mentioned above 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. 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.

Prof. Dr. Gerald Spindler