SPECTARIS Position Paper

on the European Commission's Proposal for a Cyber Resilience Act (CRA)

Felix Dotzauer
Regulatory Affairs Manager

SPECTARIS • German Industry Association for Optics,
Photonics, Analytical and Medical Technologies

Werderscher Markt 15
101117 Berlin
Fon: +49 30 414021-10
Fax: +49 (0)30 41 40 21-33

regulatoryaffairs@spectaris.de
www.spectaris.de

I. Executive Summary

In times of constantly changing and increasing cyber threats and risks, regulatory actions to improve the general cybersecurity level of digital products, companies and infrastructures on a European level are of the highest importance. SPECTARIS therefore welcomes the European Commission's proposal for a Cyber Resilience Act (CRA) that would introduce horizontal and risk-based cybersecurity requirements for digital products in the European Union based on the New Legislative Framework (NLF). In connection with the recently adopted NIS2 Directive, which demands a heightened cybersecurity baseline for critical infrastructure, the CRA could provide a coherent, transparent, and adaptable cybersecurity framework within the European Union.

However, to achieve this, SPECTARIS and its member companies – German manufacturers from the Optics, Photonics, Analytical and Medical Technologies – see clear areas of improvement for the planned legislation. In the hope that the European institutions will take our views into account, we point out the following key issues in the current proposal:

- **Avoiding regulatory overlap and redundancies:** As the CRA is part of the vast regulatory mosaic regarding digitalisation in the EU, the proposed text recognizes the relevance of other horizontal legislation. We stress the importance of providing a clear interplay between requirements of the CRA and other EU legislation, such as the NIS2 Directive, the AI Act, the Machinery Regulation and the Radio Equipment Directive, to minimize the risk of regulatory overlapping, redundancies and/or fragmentation. This will substantially increase legal certainty for economic operators that fall under the CRA's scope.
- **Keeping medical devices & in vitro diagnostics out of scope:** Legislators must ensure that products covered by Regulation (EU) 2017/745 (MDR) and Regulation (EU) 2017/746 (IVDR) are fully exempted and that sectoral legislation for medical devices and in vitro diagnostic medical devices (IVDs) prevails. It must be ensured that medical devices and in vitro diagnostics are not indirectly in scope of the CRA due to cross references to other horizontal legislation (e.g., via the AI Act or EHDS Regulation). This is of vital importance to avoid inconsistencies and additional regulatory burden for an industry that is already heavily regulated and stands at maximum regulatory capacity.
- **Increasing reporting periods:** The currently proposed 24-hour time limit to report known and exploited vulnerabilities to ENISA is too short and rather unrealistic, as it does not take into account the necessary efforts for setting up such reports. Instead, we propose to increase the time frame to 72 hours, thus aligning reporting obligations with NIS2 provisions.
- **Allowing more time for implementation:** SPECTARIS urges legislators to provide a staggered application and implementation period. Rather than providing one fixed timeline for implementation, we propose to establish system readiness first, followed by an implementation period for economic operators. Successful implementation of the new requirements by economic operators hinges upon the necessary structural elements such as third-party conformity assessment bodies to be sufficient, available and ready to act. Only then a fixed time for implementation should be defined. This will not only provide European and national authorities with more time, but also avoid constant delays in implementation. It would also give companies much-needed time to set up the

necessary procedures and structures to comply with CRA requirements, which is especially important for heavily regulated industry sectors and SMEs. The suggested staggered approach for implementation would, furthermore, be beneficial for much-needed standardisation efforts, since the current timetable for CRA implementation will most likely be too short for establishing harmonised standards in due time.

- **Clarifying product criticality:** The risk-based classification of products with digital elements is an essential cornerstone of this proposal. However, more clarification on the exact demarcation between risk classes is necessary. We also suggest to focus more on the actual use scenario as a variable for product criticality, instead of only product-based categorisations.
- **Preventing certification bottlenecks:** We urge legislators to draw from the recent lessons learned from implementing MDR and IVDR: Limited capacities of national competent authorities and notified bodies need to be considered. Moreover, notification processes as well as third-party conformity assessments themselves need to be implemented in an efficient way to prevent market access restrictions for digital products due to certification bottlenecks. In this spirit, we also propose to focus on harmonised standards as the main pathway for class I products with digital elements to obtain conformity. Additionally, conformity assessment fees and the amount of time necessary for the services should be made transparent, so that manufacturers are able to estimate overall costs as well as the duration of the procedure.

More detailed feedback on these issues, as well as on other areas for potential improvement, are presented in the following section.

II. Detailed feedback

Article 2 / Recital 12 – Scope

In its proposal, the European Commission clearly and unequivocally exempts products with digital elements covered by MDR and IVDR. SPECTARIS welcomes this exemption of medical devices and in vitro diagnostics (IVDs) from CRA requirements. As rightly stated in Recital 12, essential cybersecurity requirements and guidance already exist in these industry sectors. Extensive sectoral law already covers obligations for manufacturers, e.g., on risk management, security-by-design, privacy, maintenance during the product's lifecycle as well as clear provisions for instructions for use (IFU), post-market surveillance (PMS) and incident response, thereby fulfilling or even going beyond CRA requirements.

We fully support MDR/IVDR exemption. Nevertheless, there remains a question mark and potential uncertainty for manufacturers: This is due to the possibility of certain devices with digital elements falling under the proposed AI Act (as a high-risk system) or the planned EHDS Regulation (as an Electronic Health Record system), which could potentially bring the device in question back into the CRA's scope (see also Articles 8 and 24; Recitals 29 and 31). Clarification is thus needed that medical devices and in vitro diagnostics remain out of scope, despite cross references to other horizontal EU legislation. We urge legislators to address such regulatory overlaps in order to ensure proper MDR/IVDR exemption.

Article 5 / Annex I – Requirements for products with digital elements

SPECTARIS appreciates the introduction of essential requirements for products with digital elements according to Article 5 and Annex I to increase the general level of cyber resilience. Nevertheless, CRA obligations need to be adequate and fair, especially if one considers the limited resources of SMEs. Moreover, requirements listed in Annex I need to be held at a realistic baseline: It is stated that products with digital elements "shall be delivered without any known exploitable vulnerabilities" (Annex I, Section 1(2)). As other actors could be aware of vulnerabilities that the manufacturer, despite their best efforts and a high degree of preparation, does not know of, we suggest to change this wording to "any exploitable vulnerabilities known to the manufacturer" to provide a requirement that is more fitting to IT security in practice.[1] Furthermore, for an improved mitigation of vulnerabilities, it is necessary that European and national institutions share their knowledge and information on security issues with manufacturers.

Article 6 / Annex III – Critical products with digital elements

The risk-based approach in the European Commission's proposal offers some examples and orientation on what kind of products will be deemed as critical (Class I or II) or highly critical. Since Annex III and the official CRA factsheet only list a selection of potential class I or II products, and highly critical products are yet to be defined, we emphasize the need to clarify the risk classes and their demarcations to gain a better understanding. A risk-based approach can only work when manufacturers can clearly assign their products to the according risk class. Additionally, the already listed product types are often too broad and the specific intended use or environment of the product does not seem to be taken into account. Hence, for the ongoing legislative process, we suggest to focus more on intended use as a factor when determining critical product classes.

Furthermore, Article 6(4) refers to necessary conformity assessment procedures for class I and II products as stated in Article 24(2) and (3). However, based on the current proposal, class I products are not necessarily subject to a conformity assessment, if applicable standards can prove conformity (see also Article 18(4)). We would like to point out this inconsistency in Article 6(4) and suggest adding the option of relying on an applicable standard for class I products.

Article 8 / Recital 29 – High-risk AI systems

When it comes to products that are classified as both high-risk AI system and critical product with digital elements as mentioned in Article 8(3), SPECTARIS stresses the importance of providing a clear interplay between the forthcoming AI Act and CRA to avoid duplicated conformity assessments. In this spirit, a swift and efficient notification process of notified bodies designated under the CRA and AI Act is of the highest importance to ensure that manufacturers of said products can find a notified body to perform the conformity assessment.

Article 11 – Reporting obligations of manufacturers

In its proposal, the European Commission suggests that manufacturers shall report any actively exploited vulnerability or incident having impact on their product to ENISA within 24 hours. Establishing ENISA as the singular agency to report to is to be commended, since this will decrease the bureaucratic burden for companies that are operating in

[1] This suggestion is also in line with German industry position. See: *BDI Position* on CRA: [https://english.bdi.eu/publication/news/cyber-resilience-act/]

multiple EU member states. Nevertheless, we urge legislators to increase the time limit for incident and vulnerability reporting from 24 to 72 hours. This would, firstly, sensibly align with obligations in the NIS2 Directive, where the timeframe to submit incident reports is set to 72 hours. Secondly, gathering all of the necessary information as well as directly addressing vulnerabilities or incidents are highly complex and time-consuming procedures, especially from an SME perspective. Thus, raising the ceiling for reporting obligations would – in line with NIS2 provisions - provide manufacturers with much-needed time. Moreover, we ask for clarification on the timeframe of reporting "without undue delay" (Article 11) and its distinction to providing security updates or patches "without delay" (Annex I, Section 2(2) and (8)).

Article 18 – Presumption of conformity / Article 19 – Common specifications

SPECTARIS appreciates the high prioritisation of harmonised standards to provide more legal certainty (Article 18). Setting up common specifications – as stated in Article 19 – is presented as a back-up option in case of "insufficient" standards or "undue delays". It should be noted, however, that common specifications could deviate from internationally recognized standards and exclude relevant stakeholders in the process. Hence, instead of common specifications, we strongly suggest the use of harmonised state-of-the-art standards, since technical issues need to be addressed on a broad basis of stakeholders and experts searching for consensus.[2] Moreover, we ask the Commission to elaborate on what constitutes "undue delays" in this context. Unforeseen delays by themselves should not be the main argument for switching to common specifications.

Article 24 – Conformity assessment procedures for products with digital elements

Building the CRA's risk-based approach on the grounds of the New Legislative Framework (NLF) is to be commended. But as mentioned before, criticality classes of products have not been clearly defined yet. This is also the case within a class: As stipulated in Article 24(2), manufacturers of class I products with digital elements can demonstrate conformity by full application of harmonised standards - based on Article 18. Otherwise, they must carry out third-party conformity assessments. We therefore see a high degree of legal uncertainty for potential class I product manufacturers, if numerous pathways to conformity are provided. To not only offer a higher degree of legal certainty, but also decrease the risk of certification bottlenecks, SPECTARIS recommends to focus on applying harmonised standards as the main regulatory pathway for class I products.

Moreover, based on the Commission's suggestion in Article 24(4) - that EHR systems (as defined by the EHDS Regulation) should fall under the CRA's scope – we would again like to stress the importance of fully excluding products falling under MDR and IVDR. As medical devices and IVDs could potentially be classified as EHR systems, this would present a regulatory overlap that needs to be properly addressed by lawmakers.

Lastly, we welcome the emphasis of Article 24(5) on taking into account the specificalities of small- and medium-sized enterprises (SMEs) "when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs." This aspect is of great relevance for our members. In order to provide more planning security for companies with regard to the refinancing and profitability of their products, we

[2] For example, harmonised standards can be built on established international standards, such as IEC 62443 or ISO/IEC 27001.

propose to add that potential fees need to be made transparent for manufacturers. It needs to be ensured that manufacturers are able to estimate the approximate overall cost of a conformity assessment procedure where third parties are involved. Otherwise, the lack of predictibility of costs that continuously increase lead to the discontinuation of products and innovation leaving Europe. On the grounds of transparency, we furthermore suggest that notified bodies should be obliged to provide manufacturers with estimations on the processing time for conformity assessments. Such obligations should be on the grounds of a legal framework that specifies deadlines and the maximum duration of individual process stages for notified bodies.

Article 33 – Notification procedure

As mentioned before, we support the common NLF approach for the Cyber Resilience Act. Notification of conformity assessment bodies needs to be thorough, yet efficient, so that manufacturers can easily find CRA-notified bodies. SPECTARIS notes that the European Commission needs to review the lessons learned from MDR implementation, where only a limited number of notified bodies was eligible at the date of application due to notification delays. This would currently lead to an industry- and innovation-threatening certification bottleneck and the risk of medical device shortage in the EU – a risk that has recently been recognized by the Commission, and which will now be tackled with new legal and additional changes.[3]

To prevent such retrospective course corrections in the first place, it is of vital importance to provide an efficient framework, so that a sufficient number of notified bodies will be directly available from the date of application. Additionally, we suggest to create an equally efficient framework for conformity assessments themselves, as this lowers the risk of certification backlog.

Article 57 – Entry into force and application

An implementation period of 24 months (or 12 months for reporting obligations) after entry into force is a rather ambitious undertaking. For such an extensive, horizontal and complex legal framework, manufacturers will have to review, renew and/or set up new IT security structures and procedures, which undoubtedly will be a very tedious and time-intensive task. Moreover, capacities for notification and market surveillance by national competent authorities as well as the preparedness level at ENISA will surely need to be increased to provide a stable and well-functioning CRA framework. This is also the case for notified bodies that need time to adapt to a new certification regime, especially when considering the continuing shortage of IT and Regulatory Affairs professionals. Moreover, establishing state-of-the-art harmonised standards will most likely take longer than the suggested 24 months, as current experiences from other legislative procedures – such as MDR or the AI Act – show.

Thus, we recommend to apply a staggered approach for application and implementation: Rather than providing one fixed timeline for implementation, we propose to establish system readiness first, followed by an implementation period for economic operators. Successful implementation of the new requirements by economic operators hinges upon the necessary structural elements such as third-party conformity assessment bodies to be sufficient, available

[3] The European Commission confirmed the looming certification backlog for medical devices and the urgent need for MDR amendments in January 2023. See: *Proposal for a Regulation amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards the transitional provisions for certain medical devices and in vitro diagnostic medical devices* [https://health.ec.europa.eu/system/files/2023-01/mdr_proposal.pdf]

and ready to act. Only then a fixed time for implementation should be defined. We again underscore the importance to consider the lessons learned from MDR and IVDR implementation: Various delays in establishing the readiness of the MDR and IVDR systems led to a high degree of legal uncertainty for economic operators. In the context of the CRA, such a scenario can only be avoided with a realistic timeframe to achieve overall system readiness first, without pre-defining implementation periods from the get-go.

SPECTARIS welcomes the proposed Cyber Resilience Act and regards it as important groundwork for increasing the cyber resilience level of the European Union. When it comes to cybersecurity, the CRA has the potential to provide a functioning framework for products with digital elements, if the above-mentioned issues will be addressed properly. In any case, SPECTARIS and its members always stand ready for an open and constructive dialogue with policymakers, both on a European and national level.