VDA German Association of the Automotive Industry

Position

Implementation of the NIS2 Directive in national law

Berlin, March 2023

1 Introduction

The German automotive industry welcomes the conclusion reached in the trilogue negotiations on the “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high level of common cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148” (the NIS2 Directive). In conjunction with the Cyber Resilience Act very recently proposed by the European Commission, and the Resilience of Critical Entities (RCE) Directive that has already been passed, NIS2 will bring about a lasting improvement in Europe’s digital resilience. The VDA calls on the German Government to transpose the NIS2 Directive rapidly into national law, and to take account of the interplay of the various related regulations. This process should increase protection against both digital and analogue threats by taking a holistic approach, intensify cooperation between the state and the business sector in order to protect Germany as an industrial location, establish efficient processes, and introduce requirements appropriate to the risks. Furthermore, implementation of NIS2 within the European Union should be a largely coordinated process of transposition into national law by the Member States. The German automotive industry is active in many parts of the European Union, and cybersecurity can only be enhanced if the regulatory conditions are harmonized throughout the EU.

Most recently, a large number of towns/cities and districts have been victims of large-scale cybersecurity incidents. They have prevented both citizens and businesses from using important administrative services – in some cases for several months. The German automotive industry depends on the public administration functioning well at all times, e.g. the planning and approval procedures. The far-reaching expansion of the scope of NIS2 means that the regulations will now apply to medium-sized enterprises with more than 50 employees or with an annual turnover exceeding ten million euros. So now also municipalities, districts and towns/cities must be obligated to implement cybersecurity measures appropriate to the risks. We call on the German Government to include the public administration at all levels of the federal state in the scope of the new law, to ensure that all authorities implement risk-appropriate cybersecurity measures and thus improve protection of sensitive data from cybercriminals.

Merging the corporate categories in NIS2 and the German IT Security Act 2.0

For the sake of clear standards, no new categories of enterprises should be introduced during the implementation of NIS2. Instead, the “essential entities” and “important entities” should be merged with the existing categories in German law of “critical infrastructures,” and “companies in the special public interest” (known as “UBI”). Furthermore, division into the categories UBI 1 to 3 should be abolished and in the future the sector in which a company operates should be the sole factor determining whether it comes under the German law implementing NIS2. The current category UBI 1 should be regarded as a sector within the scope of the new German law, alongside the sectors defined in NIS2 itself.

It is absolutely essential that the following points are considered when the scope of the German and the European cybersecurity laws is merged:

- Push forward European harmonization: the German Government should align implementation as closely as possible with the scope of NIS2 and not introduce or perpetuate any additional sectors in Germany. (Sub)sectors that are not listed as critical subsectors at European level should be removed from the scope of the German implementation law. This would affect, for example, the logistics sector that at present falls under the Act on the Federal Office for Information Security 2009 (‚BSIG'), and which from a European viewpoint is – correctly – not regarded as a separate critical category in NIS2.

- Complete elimination of system-based thresholds: in contrast to the approach taken to date in the 'KRITIS Regulation' of the Federal Office for Information Security (BSI), in which system size determines whether companies fall within the scope of the regulation, in the future – according to the NIS2 logic – company classification should depend solely on the size of the company (number of employees and annual turnover).

- Pursuant to Annex 1, section 1 a) last indent, "operators of charging stations" count as essential entities. A broad interpretation would classify companies as "essential entities" if they operate at least one (1) charging station for their employees or – for instance – for customers (e.g. charging pillars in front of supermarkets). This would include a very large number of companies; obviously that cannot be the intention. It should therefore be made clear that only those companies are to be classified as essential entities whose primary business purpose is to operate charging stations.

2 International and overarching alignment of reporting obligations

NIS2 includes a reporting obligation on the companies concerned. National implementation of NIS2 by the 27 EU Member states could result in the industry submitting to the national authorities multiple reports that differ in part. The German Government should ensure that companies only have to submit a report in one Member State, and not in all of them. This will also reduce the amount of work for the national authorities which would otherwise have to receive and process the same information multiple times as data is exchanged internationally.

The EU General Safety Regulation already obliges the automotive industry to report to the national authorities. Here, too, the German Government should avoid creating an obligation to report the same aspects to different national authorities.

3 Framework for administrative fines differentiated by the severity of the infringement

When the new amounts of administrative fines are introduced, they should be much more differentiated and adapted to the various infringements than is the case at present with the universal upper limits pursuant to Article 34(3) and (4) of the NIS2 Directive. The VDA is generally in agreement with the introduction of fines as penalties for non-compliance with legal requirements. However, the amount of the administrative fine should always be proportionate to the infringement. Furthermore, it should be impossible to impose multiple fines for the same actions (e.g. actions violating both the GDPR and NIS2).

Severe penalties for companies that act unlawfully hinder rather than promote transparency concerning current attack vectors. Therefore, the principles elaborated for criminal law should be applied to determine the appropriate administrative penalty in the context considered here.

4 Introduce unified, Europe-wide security requirements such as the CSA system

For NIS2 to exert its full effect, we call on the German Government to define security measures in the closest possible coordination with its European partners. Numerous essential and important entities not only engage in cross-border activities, but are part of a larger ecosystem with mutual dependencies along the value chain. Many of their suppliers provide services that are offered in several sectors. Therefore in the Council, national governments should coordinate the implementation of NIS2 as closely as possible. The greatest possible regulatory consistency across Europe can make the entire EU even more cyber-resilient. At the same time, this can make corporate implementation more efficient.

Products with cyber-resilience appropriate to the risks are an essential prerequisite for the implementation of technical cybersecurity measures. The VDA therefore explicitly supports the introduction of horizontal cybersecurity requirements for products with digital elements and of vulnerability management under the Cyber Resilience Act (CRA).

Nonetheless, vehicles should be excluded from the NIS2 Directive pursuant to Regulation (EU) 2019/2144 [on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles], as is the case with the CRA.

For vehicles, at least equivalent cybersecurity requirements already exist under Regulation (EU) 2019/2144 [on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles]. It should therefore be made clear that in the NIS2 Directive (as in the CRA) Regulation (EU) 2019/2144 is recognized as a “sector-specific” regulation and the requirements of NIS2 (IT Security Act 3.0) do not apply either to vehicles or to vehicle services.

5 Possibility of verifying the trustworthiness of employees

Protection against digital risks is possible only with a combination of technical, organisational and personnel measures. The wide-ranging organisational, operational and technical measures, which essential and important entities will have to implement pursuant to Article 21 of the NIS2 Directive to strengthen their cyber resilience, will amount to nothing if they are performed by employees (of whatever origin) who intend/are instructed to harm the company.

To minimize the threat from internal saboteurs and to boost the efficacy of organisational, operational and technical cybersecurity measures, for the purpose of comprehensive, anticipatory economic protection security clearance checks should be possible for companies that are not supervised by the Federal Ministry for Economic Affairs and Climate Action within the meaning of the German Security Clearance Check Act [Sicherheitsüberprüfungsgesetz, SÜG]. In the future, all companies to which the German law implementing NIS2 applies should have the possibility of applying to the competent offices for security clearance checks on employees whose functions are relevant to security. It is absolutely essential that the German Government introduces such a possibility in the law implementing NIS2. It is not expedient to focus exclusively on technical security.

Companies should also be given the possibility of investigating the trustworthiness of employees and job applicants in especially security-sensitive areas. In the future, procedures must also be established for including foreign staff in the security checks. Processing times should also be reduced. Waiting periods of several months for security clearance checks, as currently occur, hold back the economy and do not improve security.

6 Add representatives of essential and important entities to UP KRITIS

All businesses that will fall within the scope of the cybersecurity legislation as essential or important entities should have the possibility of participating in the implementation plan for KRITIS (called “UP KRITIS”). Structured inclusion in UP KRITIS of the companies now being added to the scope of the cybersecurity legislation can greatly facilitate the exchange of information on current security incidents and on implementation of technical and organisational measures. Moreover, the manufacturers of products and systems used by essential entities must be much more closely involved in these discussion formats.

7 Let business develop the state-of-the-art, instead of defining it in the legislation

In the future determining what the “state-of-the-art” is, and issuing implementing acts on this basis, should not be the job of the European Commission or national authorities. Instead, recognized standards and specifications elaborated by the business sector and tried-and-tested sector-specific rules for the automotive industry must be implemented. They will be continually updated by the relevant expert groups and will therefore reflect the real state-of-the-art – a regulatory requirement would never be able to do this in the same way, because of the lengthy administrative procedures that would be involved. In addition, the requirements placed on the state-of-the-art developed in this manner will already be in line with implementation instructions and regulations. This is the only way to secure the necessary flexibility and fast reactions to changes.

8 Interrupt further implementation of the IT Security Act 2.0

In view of the approaching implementation of the NIS2 Directive in national law, the German Government should interrupt the further implementation of requirements from the IT Security Act 2.0 which have not yet been applied. In particular, the German Government should no longer push forward the introduction of companies in the special public interest in category II (“UBI 2” – domestic value creators and their suppliers) under section 2(14)(2). The additional effort required from the companies concerned to satisfy the regulations, which would arise from consecutive implementation of section 8(f) of the BSIG and then NIS2, would be out of all proportion to the resulting marginal improvement in cyber resilience.

9 Provision of and legal framework for implementation / orientation assistance

In the context of the NIS2 Directive and its transposition into national law, the legislator should provide sufficient specific implementation / orientation aids concerning the law in good time.
In the best case scenario, they would be provided simultaneously when the new domestic law implementing NIS2 enters into force. Furthermore, the legal framework for these aids should be made unequivocally clear, i.e. it must be clear to the entities affected whether they represent mere aids / orientations, or whether the law demands their implementation in full. Such implementation / orientation aids do actually exist in the current KRITIS context in Germany, but it is not clear whether they are legally binding on the companies concerned.

10 Establish efficient, fully digital registration and reporting

Maintaining an appropriate level of effort for complying with the terms of Article 23 of the NIS2 Directive relating to registration and reporting of incidents requires the introduction of an efficient, fully digitized registration and reporting system based on the once-only principle. Since the German IT Security Act was introduced, companies defined as operators of critical infrastructure have had to register with the BSI. The IT Security Act 2.0 expanded this requirement to include companies in the special public interest. In the future, the NIS2 Directive and the Resilience of Critical Entities Directive will require even more companies to register with the BSI, and many of them with the Federal Office for Civil Protection and Disaster Assistance as well. These registration obligations should be combined in an efficient and fully digitized process to foster a user-oriented public administration. The responsible governmental offices should have access to the registration data submitted subject to the need-to-know principle. This would reduce the effort needed to comply with the regulations, correlate registrations centrally, and free up capacities at the companies to increase protection against threats.

The reporting system also urgently needs an efficient, fully digitized procedure for the standardized and correlated recording of relevant incidents in a central system. The NIS2 Directive envisages that companies will have to file at least three to five reports per cybersecurity incident. We call on the German Government to establish a reporting system in collaboration with the business sector, through which companies can directly fulfil all their reporting obligations arising from the NIS2 and RCE/CER Directives, plus existing sector-specific reporting obligations. All the competent authorities at national, federal-state and municipal levels – including the Federal Office for Information Security, the Federal Office of Civil Protection and Disaster Assistance, and the criminal investigation offices and regular police forces of the federation and the federal states – should have access to the information submitted in accordance with the need-to-know principle. In consultation with the other EU Member States, the German Government must also ensure that companies falling within the scope of Article 26 have to report cybersecurity incidents in one Member State only. The Member States should secure among themselves a suitable form for the flow of information about such incidents, without this generating extra work for the economic players affected. This is especially important for the subcategory of number-independent interpersonal communications services (NI-ICS) provided by the publicly accessible electronic communication services pursuant to Article 26(1)(a). These services are provided over the internet and are generally available throughout Europe. As such, they have a lot in common with the digital infrastructures and digital service providers specified in Annex I section 8 and Annex II section 6. However, in this case responsibility is not determined geographically by the location of the providers' main office within the EU, but by where they supply their services. As such, they will probably be subject to 27 different registration and reporting obligations instead of one single one. The Cooperation Group should ensure that such providers have to report only to a single authority, coupled with additional exchange of information between the Member States.

Furthermore, during follow-up reporting companies should always have access to the information previously submitted and be able to add to and correct it, instead of having to start from the beginning every time. In addition, the BSI and the Computer Security Incident Response Teams (CSIRTs) should request an intermediate report only in exceptional cases under Articles 24 and 23(4)(c). In view of the expanded scope of application to include medium-sized companies, and the concomitant acute shortage of IT security experts, numerous companies will be unable to fulfil the applicable obligations within the legally defined periods unless a unified and lean digital reporting channel is available.

Contact persons

Dr. Marcus Bollig
Managing Director
marcus.bollig@vda.de

Martin Lorenz
Acting head of Department Automotive Technologies and Eco-systems
Head of Coordination Unit for Security & Data

martin.lorenz@vda.de

The German Association of the Automotive Industry (VDA) consolidates more than 650 manufacturers and suppliers under one roof. The members develop and produce cars and trucks, software, trailers, superstructures, buses, parts and accessories as well as new mobility offers.

We represent the interests of the automotive industry and stand for modern, future-oriented multimodal mobil-ity on the way to climate neutrality. The VDA represents the interests of its members in politics, the media, and social groups. We work for electric mobility, climate-neutral drives, the implementation of climate targets, securing raw materials, digitization and networking as well as German engineering.

We are committed to a competitive business and innovation location. Our industry ensures prosperity in Germany: More than 780,000 people are directly em-ployed in the German automotive industry. The VDA is the organizer of the largest international mobility platform IAA MOBILITY and of IAA TRANSPOR-TATION, the world's most important platform for the future of the commercial vehicle industry.

If you notice any errors, omissions or ambiguities in these recommendations, please contact VDA without delay so that these errors can be rectified.

Publisher	German Association of the Automotive Industry Behrenstraße 35, 10117 Berlin www.vda.de/en
Copyright	German Association of the Automotive Industry Reprint, also in extracts, is only permitted, if the source is stated.
Version	March 2023

@VDA_online
Verband der Automobilindustrie

VDA