VDA Verband der Automobilindustrie

Position

Input from associations on implementing the NIS 2 Directive

May 2024

1. VDA's recommendations concerning the draft bill

Registration obligations
- For companies operating in more than one EU Member State, a single national certification should be sufficient.
- CRITIS operators must also register with the BSI and the Federal Office of Civil Protection and Disaster Assistance (BBK).
- Business associations should be able to support companies that are affected.

Notification obligations
- The NIS 2 Directive increases the number of notifications and their requirements. An efficient, digitized notification portal should be established.
- In most cases the Federal Office for Information Security (BSI) should refrain from intermediate notifications, to minimize the costs of complying with the regulations.
- Affiliated companies should be able to submit joint notifications, to reduce complexity.
- Notifications should also be possible in English and to a central office (once-only principle).

Managers' liability
- The personal responsibility of the management for cyber risk management is being extended without the possibility of delegation; the VDA takes a critical view of this.
- Managing directors can be held personally liable, which represents a considerable extension of liability.

Implementation of risk management measures
- Calculation of the implementation costs to the German economy is unreliable.
- The assumption that CRITIS operators face no extra costs is refuted by companies affected.

Abolition of the category "companies in the special public interest"
- Abolishing this category will simplify and clarify the orientation of the cybersecurity regulation.

Sectors
- Companies find it difficult to determine whether they are affected pursuant to Annexes I and II of the NIS 2. Particular uncertainty exists in sectors such as "digital infrastructure" and "ICT service management."

Chief information security officer (CISO)
- The option of establishing a CISO for each entity affected, who has to be appointed upon registration.

Possibility of checking employees' trustworthiness
- Employees are the main target of cyberattacks; technical, organizational and operational measures must therefore be supplemented. Companies should be able to apply for security checks on their employees.

Omission of public administrations
- Public administrations of the *Länder* (federal states) and the municipalities should be included in the scope of application, as they provide essential administrative services.

1. Introduction

The German Association of the Automotive Industry (VDA) wishes to express its thanks for the opportunity to submit an opinion on the current draft prepared by the German Federal Ministry of the Interior and Community (BMI) for a law to implement the NIS 2 Directive and regulate fundamental features of information security management in the federal administration (NIS 2 Implementation and Cyber Security Strengthening Act, NIS2UmsuCG) of May 7, 2024. We welcome the fact that implementation of the NIS 2 Directive will bring about the expansion and relevant adaptation of the regulatory framework created by the German Act on increasing the security of IT systems (IT Security Act) of 2015 and the IT Security Act 2.0 of 2021.

As a result of implementation, new requirements in particular will be introduced for certain companies; regulations for the federal administration will also be added. In the VDA's view, crucial factors will be a holistic approach for improving protection against digital and analog threats, enhanced cooperation between the state and the private sector, and the introduction of efficient processes and risk-appropriate requirements.

Given the increase in cybersecurity incidents, which also affect numerous cities and districts, a well-functioning public administration is of great importance to citizens and the private sector, and of course for the German automotive industry as well. Expansion of the scope of application of the NIS 2 Directive already means that medium-sized companies are affected, thus obligating districts and cities to implement appropriate cybersecurity measures. We therefore call on the Federal Government to include the public administration at all levels of the federal state in the scope of application, in order to improve the protection of sensitive data against cybercriminals.
It would also be advisable for "ethical hackers" to be required for efficiently performing penetration tests, and for a corresponding justification with reference to Section 202a of the German Criminal Code (StGB) to be added to the national implementation of NIS 2. This would enable ethically motivated hackers who assist companies in identifying security loopholes to remain unpunished on the basis of such an explicit regulation.

Annex II section **5.5** of the draft bill explicitly mentions **the manufacture of motor vehicles and vehicle parts**. This draft therefore also affects the German automotive industry as a sector that is an "**important entity**."

The main changes in the current draft bill are:

- The introduction of the categories pursuant to the NIS 2 Directive markedly expands the scope of application, which until now has been restricted to operators of critical infrastructures, providers of digital services and companies in the special public interest.
- The catalog of minimum security requirements pursuant to Article 21 paragraph 2 of the NIS 2 Directive is integrated into the BSI law, whereby the intensity of the measures will be differentiated in accordance with the various categories, in order to maintain proportionality.
- The previous one-stage procedure for reporting incidents will be replaced with the three-stage system from the NIS 2 Directive, whereby the bureaucracy involved for the entities is to be minimized within the national scope for flexible implementation.

- The BSI's toolbox of instruments is being expanded with regard to the supervisory measures provided for in the NIS 2 Directive.
- The annual cost to the economy of compliance will increase by around 2.3 billion euros. A total one-off cost of around two billion euros will also be incurred. This will be incurred almost exclusively in the category of introduction or adaptation of digital process workflows.

3. Summary

Implementation of the NIS 2 Directive requires companies that are categorized as "essential" or "important" to register within three months at the latest via an official internet portal. One important measure is the automated provision of relevant information by government agencies for the companies concerned.

To minimize the administrative costs, companies with operations in more than one EU Member State should only have to present a certification to their national authority once. Affiliated companies should have the option of common registration, as they frequently use shared services and infrastructures. The VDA believes this type of joint registration would reduce costs and complexity both for the companies and for the BSI. There are no apparent disadvantages, as long as the affiliated companies are explicitly indicated as such.

In addition to the existing requirements of the German IT Security Act 2.0, more companies will have to register with the BSI and in some cases also with the BBK, when the NIS 2 and CER Directives come into force for CRITIS operators. These registration obligations should be drawn up so they are efficient and digital, to take account of the needs of the companies. Access for government agencies should be regulated in accordance with the need-to-know principle.
Bundling all the relevant information about a cyber incident in one central office would have procedural advantages regarding efficiency and effectiveness, provided that appropriate security standards are satisfied.

In view of the large number of companies affected, company and industry associations should be able to actively support them.

The NIS 2 Directive considerably expands the notification obligations. It is crucial that together the BSI, the European Commission and ENISA set up an efficient and fully digitized notification portal so that the tight notification deadlines are not further shortened as a result of multiple notifications and differing formalities.
To take account of the considerable costs of compliance, the BSI should refrain from interim notifications. Medium-sized companies in particular need their resources for addressing major security incidents. Unnecessary multiple notifications should therefore be avoided. Instead, the portfolio of advisory services should be expanded and all security authorities should be obligated to involve important entities.

The VDA supports the use of an "organization account" as the central communication interface between the state and industry. This would reduce the amount of bureaucracy involved and would be in line with the once-only principle.

Companies in a corporate group should have the option of combining notifications about a shared situation into a single common notification in order to increase efficiency and accelerate processing. Notifications should also be permitted in English to facilitate the work of the BSI and simplify the forwarding of information to international partners. The automotive industry can cope with the deadlines envisaged for the notification obligation, but they should be coordinated both at national and at international level.

It is essential to ensure both a clear regulation for cooperation and the protection of company and customer data, especially with regard to the notification and documentation obligations associated with cyber incidents. Small and medium-sized enterprises (SMEs) require straightforward, unbureaucratic implementation and application of the notification system, as they often have difficulties in satisfying the obligations within the deadlines. A central point of contact for notifications at the federal level should be set up to realize the once-only principle. The BSI could act as an interface for cooperation between the Federal Government and the *Länder*.

Section 30 of the current draft bill considerably extends the personal responsibility of the corporate management for cyber risk management. Managers can be held personally liable, in effect markedly extending the scope of liability.

The German legislation specifies no detailed requirements for companies or authorities concerning implementation of the risk management measures mentioned in Article 21 of the NIS 2 Directive, particularly with regard to criticality, sector and an entity's size. The calculation of the economic cost required is unreliable because assumptions are regarded as doubtful – such as no additional costs to CRITIS entities and 17% of entities not coming under this implementation regulation. It is urgently necessary to have a detailed implementation aid and clear expectations from the BSI, so that companies can implement the necessary measures within the deadlines. More precise derivation of the implementation costs and guidelines from the BSI would be of considerable help to the companies concerned.

Companies find it difficult to determine whether they are affected pursuant to Annexes I and II of the NIS 2 – with the exception of the automotive sector, for which this is easier. Companies can be affected in more than one sector and must indicate this during registration. There is great uncertainty in sectors such as "digital infrastructure" and "ICT service management." For example, German parent companies that offer data center services to their European subsidiaries could be categorized as "essential entities." Likewise, all entities that offer SOC (Security Operations Center) services could be NIS-2-relevant, which could also affect foreign subsidiaries. Clarification in these sectors would help the companies to make the appropriate preparations.

It should be possible to conduct security checks and design them to be efficient, whereby legal amendments to the German Federal Data Protection Act (BDSG) may be required. Sufficient resources must be made available by the state.

A "Federal CISO" will be introduced at federal (national) level. As part of NIS 2 implementation, every entity concerned could appoint a responsible CISO, similar to a data protection officer. The legislator could use the Supervisory Requirements for IT in Financial Institutions (BAIT) for orientation. The management must deploy an information security officer who is responsible for all information security matters, both internally and in dealings with third parties.

This function should be separate from operation and development of IT, to avoid conflicts of interests and to underscore the extensive remit of the information security officer.

Public administrations of the *Länder* and municipalities should also be included in the scope of application, as they provide essential administrative services.

The VDA welcomes the abolition of the category “companies in the special public interest” as this gives the cybersecurity regulation a clear orientation.
Threshold values for critical facilities should be laid down in the law itself, to guarantee transparency and ensure clear orientation for the companies affected.

Details:

4. Registration obligations

When the NIS 2 Directive is implemented, especially important and important entities will be required to register after three months at the latest (Sections 33 and 34 of the current draft bill). It is expected that there will be an official internet portal for registering. One crucial prerequisite is the automated provision of relevant information by government agencies for the companies concerned.

To minimize the administrative costs to the affected companies that have operations in other EU Member States, they should only have to present a certification to their own national authority once, which contains details of the Europe-wide corporate structure and the individual national companies, and which is accepted by the competent authorities and forwarded to the relevant authorities of other European countries.

For companies in an (affiliated) group, it should be possible to register the affiliated companies in a single common registration process. Affiliated companies usually use common services, infrastructures, systems, applications, processes and procedures. A summary of the registrations of individual affiliated companies in one common registration would reduce costs and complexity both for the companies and for the BSI. There are no apparent disadvantages of a common registration of affiliated companies, as long as the common registration explicitly indicates the affiliated companies to be registered.

In addition to the existing requirements of the German IT Security Act 2.0, the simultaneous entry into force and implementation of the NIS 2 Directive and the CER Directive for CRITIS operators will require more companies to register with the BSI and in some cases also with the BBK. These registration obligations should be adapted to the needs of the companies and drawn up to be as efficient and digital as possible. Access for government agencies should be regulated in accordance with the need-to-know principle. Bundling all the relevant information about a cyber incident in one central office would have procedural advantages regarding efficiency and effectiveness, provided that appropriate security standards for information transmission and storage are satisfied.

Owing to the large number of affected companies that is expected, in our view consideration should be given to the possibility of company and industry associations actively approaching companies and supporting them as appropriate.

Shortening the registration period in the case of changes to two weeks as compared with the period of three months specified in the NIS 2 makes the situation much more difficult for German companies and should be withdrawn.

5. Notification obligations

Against the background of the massive expansion of the notification obligations provided for in the NIS 2 Implementation and Cyber Security Strengthening Act (NIS2UmsuCG) (from one notification per incident under the IT Security Act 2.0 to up to five notifications, and from actual incidents under the IT Security Act 2.0 to possible incidents), it is of crucial importance that the BSI sets up an efficient and fully digitized notification portal in cooperation with the European Commission, the European Union Agency for Cybersecurity (ENISA) and with the involvement of the BBK. This portal should ensure that the already tight notification deadlines are not further shortened as a result of multiple notifications and differing formalities.

To take account of the considerable work involved in compliance which is associated with each notification, in most cases the BSI should refrain from an interim notification pursuant to Section 32(1) (3). While addressing a major security incident, medium-sized companies in particular will have to invest all their human and financial IT security resources in addressing the incident. It is therefore essential to prevent unnecessary multiple notifications in order to avoid creating additional burdens for the companies. Instead, the portfolio of advisory services pursuant to Section 36(1) should be expanded and all security authorities should be obligated to involve important entities.

The VDA supports the use of the “organization account” developed for the Online Access Act (OZG) as a portal solution for notification. This would considerably reduce bureaucracy in the companies, as the organization account could serve as a central communication interface between the state and the private sector. A standardized interface between the state and the private sector would also considerably bring down the implementation costs, as only one system would have to be updated and developed further. Furthermore, use of the organization account would be in line with the once-only principle.

To decrease the complexity of the notification procedure and to limit the costs incurred by the BSI and the companies affected, companies in an (affiliated) group should have the possibility of combining notifications by the affiliated companies, which describe one and the same situation and satisfy the same types of notification obligations of the individual affiliated companies, into a single common notification. The common notification will not mean that any information is lost. Instead, the creation, forwarding and processing of notifications will gain significantly in transparency, efficiency, speed and security, both at the companies affected and at the BSI.

As a concession to companies with international operations, whose cybersecurity teams frequently speak English, they should have the possibility of submitting notifications to the BSI in English. This would not only facilitate the work of the BSI, but would also simplify the forwarding of information to international partners. The proposed deadlines for the notification obligation under Section 32 should be practicable for the automotive industry. The notification obligations should however be coordinated at national and international level to ensure a smooth process.

It is essential to ensure clear regulation of cooperation and an obligation on the authorities to protect company and customer data, in particular with regard to the prescribed obligations on the companies affected to notify and document cyber incidents to the competent authorities such as the BSI and the BBK.

Given the fact that many small and medium-sized enterprises (SMEs) in the automotive industry will have difficulties in complying with the prescribed obligations within the legally defined deadlines, straightforward implementation and application of the notification system are urgently needed. Under the NIS 2 Directive (and under the CER Directive), the federal authorities should have a single point of contact for cyber incidents to enable submission of one single notification or report per incident (once-only principle). The BSI could serve as an interface for cooperation between the Federal Government and the *Länder*, and use collaborative IT applications for exchanging information and for the notification procedure. The NIS 2 imposes a reporting obligation on affected companies. The national implementation of the NIS 2 by the 27 EU Member States can lead to the industry being required to submit multiple reports, which may differ in parts, to the various national authorities. The Federal Government should ensure that companies only have to submit their reports in one EU Member State and not in all of them, to minimize the costs incurred by the companies and the authorities. A conceivable alternative would be that multinational corporate groups need only submit one notification to the European authority ENISA in the case of cross-border incidents.

The EU's General Safety Regulation already obligates the automotive industry to report to the national authorities. It should be ensured that companies are not required to report on the same aspects to several different national authorities.

6. Managers' liability

The current draft bill goes beyond the requirements of the NIS 2 Directive, in that it envisages personal responsibility of the management for monitoring the cyber risk management, in particular for especially important and important entities, without the option of delegating this responsibility to third parties (Section 38). Accordingly, business managers can be held personally liable for damage resulting from cyber risks, where recourse claims and demands for fines are concerned. The only situation in which it is permissible to waive claims for damages against the business managers or a settlement is that of insolvency. This represents a considerable expansion of the personal liability of business managers, particularly in limited liability companies (*GmbH*), which until now have had a certain amount of legal room for maneuver.

It remains unclear whether this personal liability can be insured, and what steps will be initiated by the supervisory boards, the authorities and the public prosecution service, when the managers are either not held liable for the company, or only in part (infringement of Section 38 (2)). It would be a welcome step if these points were brought out more clearly in the law and this did not require interpretation by lawyers.

7. Implementation of the risk management measures

The German legislation does not specify in detail what is expected from the companies and authorities concerning how exactly the risk management measures mentioned in NIS 2 Article 21 are to be applied in relation to criticality, sector, the size of the company or other factors.

Calculation of the cost to the German economy could provide a rough starting point for the cost of implementation. However, it does not represent a reliable source of information. For example, it is assumed that implementation of NIS 2 will not entail any extra costs for CRITIS companies. Requests for clarification from affected companies testify to the opposite. One may also seriously doubt the assumption that 17% of companies would not come under this regulation. Equating the costs involved in implementing the NIS Directive with the costs involved in implementing the NIS 2 Directive is not tenable. The only rough indication of what the legislator expects is the assumption that large important entities will incur 70% of the costs incurred by an essential entity, and moderately important entities will incur 35% of the costs incurred by an essential entity.
It is urgently necessary for the BSI to provide an implementation aid containing specific details of what is expected from the entities concerned, which covers the measures to be implemented, to enable the companies to implement them within the deadline.

A much better derivation of the implementation costs for the companies affected and BSI guidelines on the measures expected would represent significant assistance for the companies affected.

8. Abolition of the category “companies in the special public interest”

The VDA explicitly welcomes the decision to abolish the category of “companies in the special public interest,” and the resulting concentration on important and especially important entities, instead of further differentiation. This measure brings simplification and clear orientation to the field of cybersecurity regulation and contributes to harmonization at the European level. It is positive that Germany supports the path of pan-European standardization and has abandoned the special path introduced by the IT Security Act 2.0.

However, it would be desirable for the threshold values for critical systems to be determined directly in the NIS2UmsuCG, instead of referring to a downstream legal ordinance. Direct determination in the law itself would create transparency and provide clear orientation for the companies affected. This would facilitate the implementation process and enable swifter adaptation to the legal requirements.

9. Sectors

It is already difficult for companies to determine, with the aid of Annexes I and II of the NIS 2, whether they come under this regulation. This situation is easier for the automotive sector. A company can, however, belong to more than one sector and be affected in them, and these sectors must be indicated during registration.
In some sectors there is great uncertainty among the companies affected. For example, "Digital infrastructure" could apply to all German parent companies that offer their data center services to their European subsidiaries. The latter would then be "essential entities."
The sector "management of information technology and telecommunication" could theoretically apply to all entities that offer SOC (Security Operations Center) services to the European companies in their affiliated group.
This could lead to a case, for example, where an Indian subsidiary is NIS-2-relevant because of its SOC services.
Clarification in these two sectors would help the German companies to prepare for implementation as essential or important entities.

10. Chief information security officer (CISO)

A "Federal CISO" will be introduced at the federal (national) level. Implementation of the NIS 2 offers the opportunity of establishing a responsible CISO for each entity concerned, who could also be appointed during registration (similarly to the data protection officers at the data protection authorities).

The legislator can, for example, utilize the tried-and-tested provisions in the regulations for the financial sector and replicate BAIT 4.4-4.6 (Supervisory Requirements for IT in Financial Institutions): "The management board shall establish an information security officer function. This function is responsible for all information security issues within the institution and with regard to third parties. It ensures that information security objectives and measures defined in the institution's IT strategy, information security policy and information security guidelines are transparent both within the institution and for third parties, and that compliance with them is reviewed and monitored regularly and on an event-driven basis."

The requirement placed on finance institutions to separate the function of the information security officer from areas that are responsible for operation and further development of the IT systems, should also be applied here. This will rule out a situation in which the information security officer is subordinated to the head of IT. This will greatly help to prevent conflicts of interests and underscore the much more extensive remit of the information security officer, which goes far beyond IT-security issues.

11. Possibility of checking employees' trustworthiness

There is no doubt that employees are the main target of cyberattacks. The effectiveness of the technical, organizational and operational measures under the NIS 2 Directive is compromised if the personnel aspect is not given appropriate consideration as well. Alongside training courses for managers and staff pursuant to Section 38 (3), it is important to minimize potential risks. This also relates to the risk of insider threats arising from unidentified internal perpetrators, which can endanger business protection.

For this reason, all companies that fall within the scope of the NIS 2 Implementation Act should be given the possibility of requesting security checks on their employees from the relevant agencies. The legal prerequisites must be satisfied, in particular those enshrined in the German Federal Data Protection Act (BDSG), and must be adjusted if necessary. The procedures for security checks should be made more efficient and adapted to the needs of the companies. It is important that the state provide the necessary financial and human resources.

12. Non-inclusion of public administration

To date, the scope of application has not covered the public administration of the *Länder* and the municipalities to a sufficient degree. This situation urgently requires improvement, as the automotive industry is dependent on smooth public administration at all levels, which is not compromised by cyber safety incidents for a longer period. Alongside the federal authorities, the authorities of the states and the municipalities, especially approval and surveillance authorities, which process sensitive data and provide essential administrative services to especially important entities, should also be defined as "especially important entities."

Contacts

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

Timm Haußen
Expert
timm.haussen@vda.de

The German Association of the Automotive Industry (VDA) unites more than 620 manufacturers and suppliers under one roof. Its members develop and produce cars and trucks, software, trailers, bodies, buses, parts and accessories, and ever new mobility offerings.

We represent the interests of the automotive industry and stand for modern, future-oriented multimodal mobility on the way to climate neutrality. The VDA represents the interests of its members in dealings with politics, the media, and other groups in society.

We work to promote electric mobility, climate-neutral drives, the implementation of climate targets, securing raw materials, digitization and connectivity 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 employed in the German automotive industry.

The VDA is the organizer of the largest international mobility platform, the IAA MOBILITY, and the IAA TRANSPORTATION, the world's most important platform for the future of the commercial vehicle industry.

Published by	Verband der Automobilindustrie e. V.(VDA) Behrenstrasse 35, D-10117 Berlin www.vda.de
	German Bundestag Lobbying Register no.: R001243 EU transparency Register no.: 9557 4664 768-90

Last revised	May 2024