März 2026
14. Jahrg.
Seite 1 – 78

RAW

1

Recht ■ Automobil ■ Wirtschaft
Unternehmen | Technologie | Beratung

WISSENSCHAFTLICHER BEIRAT

Professor Dr. Frank Arloth, Ministerialdirektor a. D.
Andrea Czarnecki, Group General Counsel Continental AG
Professor Dr. Markus Gehrlein, Richter am Bundesgerichtshof a. D.
Karin E. Geissl, Rechtsanwältin, Attorney at Law, Freshfields
Dr. Peter Gladbach, Datenschutzbeauftragter AUDI AG
Professor Dr. Christian Heinrich, Katholische Universität, Ingolstadt
Dr. Florian Hofer, LL.M., Chief Legal and Compliance Officer, Daimler Truck AG
Dr. Uta Karen Klawitter, General Counsel AUDI AG
Nora Klug, LL.M., General Counsel Robert Bosch GmbH
Christian A. Mayer, Rechtsanwalt, Noerr
Professor Dr. Rolf-Dieter Mönning, Rechtsanwalt, Mönning Feser Partner
Professor Dr. Dr. h.c. Hanns Prütting, Universität zu Köln
Professor Dr. Jens M. Schmittmann, Rechtsanwalt, FOM Hochschule, Essen
Dr. Stefan Schröcker, Leiter Recht, Produktion und Vertrieb, BMW AG
Dr. Reinhard Siegert, Rechtsanwalt, Heuking Kühn Lüer Wojtek
Dr. Martin Wagener, Rechtsanwalt

SCHRIFTLEITUNG

Dr. Nicholas Schoch, Rechtsanwalt, Freshfields

STÄNDIGE MITARBEITER

Dr. Charlotte Harms, Paul Harenberg, Camillo v. Haugwitz

Dr. Nicholas P. Schoch
1 **Zwischen Regulierungswellen und Chancenfenstern**

Dr. Arun Kapoor und Prof. Dr. Thomas Klindt
2 **Der neue KBA-Kodex zur Durchführung von Rückrufaktionen**

Rafael Lier und Fabian Klöckler
5 **Reparatur- und Wartungsinformationen aus dem Elfenbeinturm? Teil I: Ein kritischer Blick auf Urteile und Gesetzgebung**

Rafael Lier und Fabian Klöckler
13 **Reparatur- und Wartungsinformationen aus dem Elfenbeinturm? Teil II: Nur ein kleiner Schritt in die richtige Richtung**

Dr. Moritz Becker und Stefanie Spancken-Monz
19 **Völkerrechtlicher Klimaschutz vor dem IGH – neuer Treibstoff für „Klimaklagen"?**

Dr. Reinhard Siegert
26 **In-Vehicle-Infotainment und Kartellrecht: Das Bundeskartellamt hält die „gates" offen**

Philipp Leber
31 **„Volksentscheid Berlin autofrei" – Ein neuer Impuls zur Steuerung des motorisierten Individualverkehrs**

Dr. Andreas Mann und Antje Zimmermann
37 **§ 357a BGB und die Wertminderung von Fahrzeugen – Dogmatik und Praxis**

Pinar Ciplak
43 **Cybersecurity Vulnerabilities in der Automobilindustrie – Verantwortlichkeiten und Haftungsrisiken zwischen Zulieferern und OEM**

Dr. Frederic Geber, LL.M. (Exeter)
47 **Die Leitlinien der EU-Kommission zur Anwendung des Data Act auf Fahrzeugdaten**

Julian Monschke und Dr. Andreas Daum, LL.M. (LSE)
52 **Ein neuer Goldstandard für die Cybersicherheit? Überblick über die NIS2-Vorgaben im Automotive-Sektor**

Sebastian Lutz-Bachmann, LL.M. und Dr. Charlotte Harms
60 **Unter wechselnden Vorzeichen: Ein neuer Kurs im Lieferkettenrecht**

Tobias André und Sebastian Lutz-Bachmann
63 **Diesel-Abgasemissionen auf dem unionsgerichtlichen Prüfstand: Eine (Zwischen-)Bilanz**

Christian A. Mayer, Felix Sedlmaier und Dr. Joachim Rung
71 **Überbordende Anforderungen an Emissionskontrollsysteme – eine Anmerkung zum Urteil des OVG Schleswig**

dfv Mediengruppe · Frankfurt am Main

nesses and with consumers, focusing on the scope of covered data and the modalities of access. While the guidelines provide useful clarifications, they stretch the notion of a connected service beyond the Data Act's text.

The notion of connected services used in the Data Act relies on Recital 17 of the Data Act, which requires bidirectional data exchange that affects the operation of the product's functions. The guidelines recognize this. Nevertheless, they classify (i) predictive maintenance prompts that appear on a vehicle dashboard and (ii) dynamic route optimization as connected services. These examples do not, however, alter vehicle functions; the driver retains control over longitudinal and lateral operation. Even if dynamic routing is seen as linked to a connected product (e. g., an in-vehicle navigation system), its outputs are derived information and therefore outside the Data Act's scope.

On data classification, the guidelines distinguish (i) raw data, (ii) pre-processed data, and (iii) derived or inferred information, treating only the first two as in scope of data access rights. The guidelines tie the notion of „derived or inferred information" to „entirely new" information and processing complexity, thereby adopting a narrow understanding of „derived or inferred information". By contrast, the Data Act's structure and Recital 15 support a broader view: information becomes derived once processing goes beyond making data understandable and usable. This implies that sensor fusion improving physical measurements and combinations of product data with external map data can fall out of the scope of the Data Act.

The guidelines confirm that (i) direct access to data must only be granted with regard to data designed to be retrievable and (ii) rights to indirect access only relate to readily available data, i. e. not to data that can only be made available employing disproportionate effort or cost. Although the guidelines are silent on the question, whether the Data Act stipulates a user verification requirement, data protection constraints necessitate such verification in practice.

In Germany, the draft Data Act Implementation Act designates the Federal Network Agency as the competent authority for the enforcement of the Data Act and the Federal Commissioner for Data Protection and Freedom of Information for data protection matters. If a matter concerns vehicle-related data, the Federal Network Agency and the Federal Motor Transport Authority shall consult the matter with each other.

Overall, the guidelines provide a useful basis for interpreting the Data Act in the vehicle sphere.

Julian Monschke und Dr. Andreas Daum, LL.M. (LSE)*

Ein neuer Goldstandard für die Cybersicherheit? Überblick über die NIS2-Vorgaben im Automotive-Sektor

I. Hintergrund der NIS2-Richtlinie und Zielsetzung dieses Aufsatzes

Die Mitgliedstaaten der Europäischen Union waren verpflichtet, die Vorgaben der NIS2-Richtlinie[1] bis zum 18.10. 2024 in nationales Recht umzusetzen. Wie in vielen anderen Mitgliedstaaten ist dies auch in Deutschland erst verzögert erfolgt. Seit dem 6.12.2025 gilt nunmehr ein nationales Umsetzungsgesetz, welches insbesondere das BSI-Gesetz grundlegend überarbeitet und die unionsrechtlichen Vorgaben in deutsches Recht überführt („**BSIG**").[2]

Die NIS2-Richtlinie zeichnet sich durch einen sehr weiten Anwendungsbereich aus und verpflichtet eine Vielzahl von Unternehmen zur Umsetzung umfassender Cybersicherheitsmaßnahmen.[3] Für viele Unternehmen stellte Cybersicherheit bislang kein eigenständiges rechtliches Kernthema dar. Zwar existierten bereits zuvor punktuelle regulatorische Vorgaben, etwa für Betreiber kritischer Infrastrukturen oder – mit breiter praktischer Relevanz – für alle Unternehmen, die personenbezogene Daten verarbeiten (Art. 32 DSGVO).

Cybersicherheit ist dabei als Teilbereich der Informationssicherheit zu verstehen. Informationssicherheit bezeichnet im europäischen Verständnis den Schutz aller Informationen unabhängig vom Medium hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit. IT-Sicherheit erfasst demgegenüber den auf informationstechnische Systeme bezogenen Ausschnitt. Der Begriff der Cybersicherheit wird in Europa vornehmlich im Kontext digitaler und netzwerkbasierter Bedrohungen verwendet und ist zugleich politisch und strategisch geprägt. In anderen Rechtsordnungen, insbesondere im nordamerikanischen Raum, wird Cybersecurity hingegen als umfassender Schutzbegriff genutzt, der organisatorische und technische Aspekte der Informationssicherheit einschließt.

---

* Mehr über die Autoren erfahren Sie auf S. III und IV.

1 Richtlinie (EU) 2022/2555.

2 Zur Gesetzgebungsgeschichte etwa *Schmidt*, RDi 2024, 550. Dieser Aufsatz knüpft an *Hajek Gross/Wünnerke*, RAW 2024, 117 an und vertieft die dortigen Ausführungen, insbesondere auf Grundlage von Praxiserfahrungen, die sich seit diesem Aufsatz ergeben haben.

3 Das BSIG wird in Zukunft durch das KRITIS-Dachgesetz flankiert werden, das die Anforderungen der CER-Richtlinie umsetzen wird. Adressaten sind vor allem Unternehmen der Kritischen Infrastruktur; Details werden noch in einer anzupassenden KRITIS-Verordnung geregelt. Auch wenn die konkrete Umsetzung noch abzuwarten ist, werden Unternehmen im Automotive-Sektor selten in den Anwendungsbereich fallen, da sie nach heutigem Verständnis selten Kritische Infrastruktur betreiben. Siehe dazu etwa https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-artikel.html (Abruf: 10.1.2025).

Unabhängig von regulatorischen Vorgaben wurde in der Automotive-Branche seit jeher großen Wert auf Informationssicherheit gelegt. Dies ist insbesondere dem hohen Stellenwert von Geschäftsgeheimnissen sowie dem Schutz von Entwicklungs- und Prototypendaten geschuldet. In der Praxis hat sich hierfür vor allem der TISAX-Standard etabliert, welcher wesentliche Elemente eines strukturierten Informationssicherheitsmanagements abbildet und zentrale Anforderungen der NIS2-Richtlinie teilweise bereits antizipiert.

Vor diesem Hintergrund ordnet der vorliegende Aufsatz die Anforderungen des BSIG für Unternehmen der Automotive-Branche ein und adressiert dabei vor allem die Auswirkungen auf grenzüberschreitende Konzerne. An geeigneten Stellen wird eine Referenz zur NIS2-Richtlinie gesetzt. Der Aufsatz adressiert sowohl OEMs als auch Zulieferer und legt den Schwerpunkt auf branchenspezifische Besonderheiten. Ein umfassender Überblick über die NIS2-Regulierung oder das BSIG kann und soll dabei nicht geleistet werden.

Dieser Aufsatz geht zunächst auf die Anwendbarkeit des BSIG auf Unternehmen des Automotive-Sektors ein. Daran anschließend werden die Anforderungen an das Risikomanagement dargestellt und dabei bestehende Best Practices berücksichtigt. Einen abschließenden Schwerpunkt bildet sodann die Verantwortlichkeit des Managements.

II. Anwendbarkeit der NIS2 auf OEMs

Zunächst wird dargestellt, inwieweit OEMs künftig unter das BSIG als *besonders wichtige* oder *wichtige Einrichtungen* fallen können. Die Prüfung der Anwendbarkeit dürfte dabei in drei Schritten erfolgen. Zunächst ist die territoriale Anwendbarkeit zu prüfen. Sodann ist zu prüfen, ob ein Unternehmen in einem bestimmten Sektor tätig ist. Schließlich ist zu prüfen, ob das Unternehmen bestimmte Schwellenwerte überschreitet.

Nachfolgend liegt der Schwerpunkt vor allem auf den Kerngeschäftsbereichen von OEMs. Die Beratungspraxis hat jedoch gezeigt, dass Unternehmen oftmals noch weitere relevante Einrichtungen betreiben. Dies kann etwa der Fall sein, wenn konzernintern Elektrizität hergestellt wird, eigene Banken im Konzern vorhanden sind oder digitale Infrastruktur betrieben wird. Hinsichtlich der digitalen Infrastruktur können insbesondere konzerninterne IT-Abteilungen oder Servicegesellschaften relevant sein.

1. Territoriale Anwendbarkeit und Zuständigkeiten

Zunächst wird die territoriale Anwendbarkeit und Zuständigkeit dargestellt. Trotz der praktischen Wichtigkeit ist dieses Thema bislang nicht hinreichend in der Literatur beleuchtet.

a) Territoriale Anwendbarkeit

Die territoriale Anwendbarkeit der NIS2-Richtlinie ergibt sich vor allem aus Art. 2 Abs. 1 NIS2-Richtlinie; die nationalen Gesetze folgen dabei dem Territorialitätsprinzip. Danach gilt die Richtlinie für Einrichtungen, die ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben. Maßgeblich ist dabei grundsätzlich die Etablierung der jeweiligen Einrichtung im Hoheitsgebiet eines Mitgliedstaats. Entscheidend ist, ob eine rechtliche Niederlassung in der Union besteht oder – in den ausdrücklich geregelten Fällen – ein Vertreter in der Union bestellt wurde (siehe dazu die Sonderregelungen in § 60 BSIG).

Das BSIG und die NIS2-Richtlinie folgen insoweit einem unternehmensscharfen Ansatz. Ein außerhalb der Union produzierender OEM fällt nicht allein deshalb in den Anwendungsbereich, weil er Produkte in die Union liefert. Wird die Fahrzeugfertigung vollständig außerhalb der Union vorgenommen, wird die maßgebliche Tätigkeit nicht „*in der Union ausgeübt*". Davon zu trennen ist die Frage, ob einzelne Konzerngesellschaften in der Union – etwa Vertriebsgesellschaften – eigenständig unter den Anwendungsbereich der nationalen NIS2-Umsetzungsgesetze fallen.[4] Dies dürfte im genannten Beispiel jedoch fernliegend sein, da reine Vertriebstätigkeiten regelmäßig keiner relevanten Einrichtungsart nach den Anlagen zum BSIG zuzuordnen sind. Internationale Gruppen müssen natürlich stets auch die Umsetzungsgesetze der für sie relevanten Länder im Blick haben.

b) Zuständigkeit der nationalen Behörden

Anknüpfend an die territoriale Anwendbarkeit stellt sich die Frage, welches nationale Gesetz und welche Behörde eigentlich zuständig ist. Diese Zuständigkeit der nationalen Aufsichtsbehörden bestimmt sich nach Art. 26 NIS2-Richtlinie sowie §§ 59 f. BISG und folgt grundsätzlich dem Niederlassungsprinzip. Zuständig ist der Mitgliedstaat, in dem die jeweilige Einrichtung niedergelassen ist.

Für die Abgrenzung ist zwischen unselbstständigen Zweigniederlassungen und selbstständigen Tochtergesellschaften zu unterscheiden. Unselbstständige Zweigniederlassungen ohne eigene Rechtspersönlichkeit gelten als Teil derselben Einrichtung; ihre IT-Systeme und Tätigkeiten werden der Hauptentität zugerechnet und fallen in den Zuständigkeitsbereich der Behörde des Niederlassungsstaats. Selbstständige Tochtergesellschaften mit eigener Rechtspersönlichkeit stellen demgegenüber eigenständige Einrichtungen dar und unterliegen nur dann der nationalen Aufsicht, wenn sie selbst die sektoralen und größenbezogenen Voraussetzungen erfüllen.

2. Materielle Anwendbarkeit

Nachdem die territoriale Anwendbarkeit und die Zuständigkeit der nationalen Aufsichtsbehörde geprüft sind, ist in einem zweiten Schritt die materielle Anwendbarkeit des BSIG zu prüfen. Maßgeblich ist dabei, ob ein Unternehmen einem der in der Richtlinie benannten Sektoren zuzuordnen ist.

Der nachfolgende Abschnitt stellt die materielle Anwendbarkeit anhand des deutschen BSIG dar. Dieses setzt die NIS2-Richtlinie in den relevanten Sektoren im Wesentlichen richtlinienkonform um, sodass die nachfolgende Darstellung zugleich Rückschlüsse auf die Systematik der NIS2-Richtlinie und damit andere Umsetzungsgesetze zulässt.

4 Ein Sonderfall kann weiterhin eine IT-Konzerngesellschaft sein, die ihre Leistungen (auch) in der Union erbringt.

Im Rahmen der Betroffenheitsanalyse werden regelmäßig umfassende Beteiligungs- und Konzernstrukturcharts ausgewertet. Dabei ist auch zu prüfen, ob Zwischenholdinggesellschaften oder reine Holdinggesellschaften in den Anwendungsbereich der NIS2-Regelungen fallen. Soweit diese Gesellschaften keine operativen Leistungen erbringen, fehlt es regelmäßig an einem Anhaltspunkt für ein Angebot von Waren oder Dienstleistungen in den Sektoren, welche in den Anlagen zum BSIG genannt werden. In diesen Konstellationen dürften solche Gesellschaften daher grundsätzlich nicht als besonders wichtige oder wichtige Einrichtungen zu qualifizieren sein. Dies lässt die Zurechnung von Schwellenwerten für die Size-Cap-Rule im Konzern gemäß § 28 Abs. 4 S. 1 BSIG jedoch unberührt.

a) Schwerpunkt für Automotive OEM: Hersteller von Kraftwagen und Kraftwagenteilen

OEMs im Automotive-Sektor werden in aller Regel im Sinne von Ziffer 5.4.1 der Anlage 2 zum BSIG der Branche Herstellung[5] von Kraftwagen und Kraftwagenteilen zugeordnet. Maßgeblich ist dabei, dass das jeweilige Unternehmen eine Wirtschaftstätigkeit nach Abschnitt C Abteilung 29 der NACE Rev. 2[6] ausübt. In diesen Fällen ist die materielle Anwendbarkeit der NIS2-Regelungen regelmäßig eröffnet.

Gemäß Abteilung 29 von Abschnitt C der NACE Rev. 2 ist die Herstellung von Kraftwagen und Kraftwagenteilen sehr umfassend erfasst. Sie umfasst zum einen die Herstellung von Kraftwagen und Kraftwagenmotoren (29.1 der NACE Rev. 2), die Herstellung von Karosserien, Aufbauten und Anhängern (29.2 der NACE Rev. 2) sowie die Herstellung von Teilen und Zubehör für Kraftwagen (29.3 der NACE Rev. 2). Damit wird die gesamte Wertschöpfungskette für Kraftwagen erfasst.

Hinsichtlich der Herstellung von Kraftwagen und Kraftwagenmotoren (vgl. 29.10 der NACE Rev. 2) ist insbesondere die Herstellung von Personenkraftwagen, Nutzkraftwagen, Bussen und sonstigen Kraftwagen einschließlich bestimmter Spezialfahrzeuge umfasst. Einzelne Ausnahmen ergeben sich ebenfalls aus Ziffer 29.10 der NACE Rev. 2.[7]

b) Weitere Sektoren

aa) Automotive-spezifische Sektoren

Automotive-OEMs sollten neben der Einordnung als Hersteller von Kraftwagen und Kraftwagenteilen auch weitere mögliche Einrichtungsarten nach dem BSIG prüfen. Dies macht zwar regelmäßig keinen Unterschied dahingehend, ob sie dem BSIG insgesamt unterfallen. Es kann jedoch zum einen für die Einordnung als wesentliche oder wichtige Einrichtung von Bedeutung sein. Zum anderen dürfte dies Auswirkungen auf die konkrete Ausgestaltung der Risikoanalyse haben, da der Schwerpunkt auf solchen Maßnahmen liegen kann, die die jeweils einschlägigen Einrichtungsarten spezifisch adressieren und schützen.

Für klassische Kraftfahrzeughersteller wird eine Zuordnung zur Branche des sonstigen Fahrzeugbaus (Ziffer 5.6.1 der Anlage 2 zum BSIG) nach Abschnitt C Abteilung 30 der NACE Rev. 2 regelmäßig nicht in Betracht kommen. Die dort erfassten Wirtschaftstätigkeiten betreffen überwiegend besondere Fahrzeugtypen, die außerhalb des typischen Kraftfahrzeugbaus liegen. Erfasst sind insbesondere der Schiffs- und Bootsbau (30.1 der NACE Rev. 2), der Schienenfahrzeugbau (30.2 der NACE Rev. 2), der Luft- und Raumfahrzeugbau (30.3 der NACE Rev. 2) sowie die Herstellung militärischer Kampffahrzeuge (30.4 der NACE Rev. 2).

Relevanz kann Abteilung 30 hingegen in Sonderkonstellationen erlangen, etwa bei der Herstellung bestimmter Fahrzeugarten, die nicht anderweitig genannt sind. Dies kann insbesondere bei der Herstellung von Krafträdern in Betracht kommen (30.91 der NACE Rev. 2), sofern diese Tätigkeit nicht bereits der Abteilung 29 zuzuordnen ist.

Weiterhin können aus Anlage 1 zum BSIG weitere Einrichtungsarten im Bereich des Straßenverkehrs (Abschnitt 2.4 der Anlage 1 zum BSIG) relevant sein. In Betracht kommt insbesondere der Betrieb einer Anlage oder eines Systems zur Verkehrsbeeinflussung (Ziffer 2.4.1 der Anlage 1 zum BSIG). Diese Tätigkeiten werden allerdings nicht durch Automotive-OEMs ausgeübt, sondern von öffentlichen Stellen (insbesondere Straßenverkehrsbehörden) oder von ihnen beauftragten Unternehmen. Ebenfalls genannt ist der Betrieb eines intelligenten Verkehrssystems im Sinne von § 2 Nr. 1 des Intelligente-Verkehrssysteme-Gesetzes (Ziffer 2.4.2 der Anlage 1 zum BSIG), der jedoch ebenfalls nicht von Automotive-OEMs, sondern regelmäßig von der zuständigen öffentlichen Straßenbaulast- bzw. Verkehrsbehörde verantwortet wird.

Darüber hinaus können Automotive-OEMs auch in weiteren Sektoren tätig sein, etwa in der Herstellung elektrischer Ausstattung oder in der Herstellung von Computer-, Elektronik- und Optikprodukten. Diese Sektoren werden im nachfolgenden Abschnitt C vertieft dargestellt.

bb) Weitere möglicherweise einschlägige Sektoren

Unabhängig von diesen automotive-spezifischen Vorgaben finden sich in großen Unternehmensgruppen häufig zentrale IT-Abteilungen oder ausgelagerte Tochtergesellschaften, die konzernintern IT-Leistungen[8] erbringen. Dies kann dazu führen, dass ein Automotive-OEM – je nach Ausgestaltung der IT-Leistungserbringung – als Anbieter von Cloud-Computing-Diensten (Ziffer 6.1.4 der Anlage 1 zum BSIG[9]), als Anbieter von Rechenzentrumsdiensten (Ziffer 6.1.5 der Anlage 1 zum BSIG[10]) oder als Managed Service Provider beziehungsweise Managed Security Service Provider (Ziffern 6.1.1 und 6.1.2 der Anlage 1 zum BSIG[11])

5 Siehe zu diesem Begriff noch unter Abschnitt C.I.2.

6 Abrufbar unter https://ec.europa.eu/eurostat/de/web/products-manuals-and-guidelines/-/ks-ra-07-015 (Abruf: 6.1.2026).

7 Etwa landwirtschaftliche Zugmaschinen, geländegängige Muldenkipper oder Panzer.

8 Dazu *Hessel/Callewaert/Schneider*, RDi, 208, 211.

9 Definiert in § 2 Nr. 4 BSIG als „*ein digitaler Dienst, der auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn die Rechenressourcen auf mehrere Standorte verteilt sind*".

10 Definiert in § 2 Nr. 35 BSIG als „*ein Dienst, der Strukturen umfasst, die dem vorrangigen Zweck der zentralen Unterbringung, der Zusammenschaltung und dem Betrieb von IT- oder Netzwerkausrüstungen dienen, und die Datenverarbeitungsdienste erbringen, mitsamt allen benötigten Anlagen und Infrastrukturen, insbesondere für die Stromverteilung und die Umgebungskontrolle*".

11 Definiert in § 2 Nr. 25 und 26 BSIG als ein „*ein Anbieter von Diensten im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten*

zu qualifizieren ist. Hinsichtlich der Einordnung als Managed Service Provider beziehungsweise Managed Security Service Provider ist nach der Rechtsauffassung des BSI[12] davon auszugehen, dass auch konzerninterne Dienstleistungen die Tatbestandsvoraussetzungen erfüllen. Maßgeblich ist, dass der zentrale IT-Betrieb eines Unternehmensverbunds organisatorisch bei einer eigenen Einheit angesiedelt ist. Ein externes Anbieten der betreffenden Dienstleistungen gegenüber Dritten ist hierfür nicht erforderlich.

Hinsichtlich eines Rechenzentrums kann eine Ausnahme für eigene Rechenzentren nutzbar gemacht werden. Nach Erwägungsgrund 35 NIS2-Richtlinie sollte der Begriff „Rechenzentrumsdienst" jedoch *„nicht für interne Rechenzentren [gelten], die sich im Besitz der betreffenden Einrichtung befinden und von der betreffenden Einrichtung für eigene Zwecke betrieben werden"*. Ob dies auch für Gruppen-weite Rechenzentren gilt, ist bislang nicht abschließend geklärt. Die englische Sprachfassung lässt diese Interpretation jedoch zu.

Schließlich kommt in Betracht, dass ein Automotive-OEM auch eine Forschungseinrichtung im Sinne von Ziffer 7.1.1 der Anlage 2 zum BSIG betreibt. Als Forschungseinrichtung gilt gemäß § 2 Nr. 12 BSIG eine „*Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung durchzuführen, um die Ergebnisse dieser Forschung für kommerzielle Zwecke zu nutzen. Bildungseinrichtungen gelten ausdrücklich nicht als Forschungseinrichtungen*". Ein Schwerpunkt der Prüfung liegt dabei auf der Frage, ob eine Einrichtung das „primäre" Ziel der Forschung verfolgt.

3. Size-Cap Rule

Wie § 28 BSIG vorgibt, ist es für die Anwendbarkeit der NIS2-Umsetzungsregelungen grundsätzlich erforderlich, dass bestimmte Schwellenwerte überschritten werden. Dies gilt vorbehaltlich der in § 28 Abs. 1 und Abs. 2 BSIG geregelten Ausnahmen.

a) Relevante Schwellenwerte

Demnach sind besonders wichtige Einrichtungen solche, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, einer der in den Anlagen zum BSIG genannten Einrichtungsarten zuzuordnen sind und a) mindestens 250 Mitarbeiter beschäftigen oder b) einen Jahresumsatz von über 50 Millionen Euro sowie zugleich eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen. Wichtige Einrichtungen sind solche Einrichtungen, die einer der in Anlage 1 oder Anlage 2 zum BSIG genannten Einrichtungsarten zuzuordnen sind und a) mindestens 50 Mitarbeiter beschäftigen oder b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.

b) Kriterium der Vernachlässigbarkeit

Der deutsche Gesetzgeber hat mit § 28 Abs. 3 BSIG einen weiteren relevanten Abweichungstatbestand aufgenommen.[13] Danach können bei der Zuordnung zu einer Einrichtungsart nach den Anlagen 1 und 2 solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der jeweiligen Einrichtung *vernachlässigbar*[14] sind. Nach den Gesetzgebungsmaterialien soll diese Regelung dazu dienen, unbillige Härten zu vermeiden.

Dieser Ausnahmetatbestand ist in der NIS2-Richtlinie selbst nicht angelegt und findet dort keine unmittelbare Entsprechung. Entsprechend wurde die Regelung im Gesetzgebungsverfahren von Fachkreisen kritisch begleitet. Insbesondere wurde darauf hingewiesen, dass die Richtlinie eine solche Relativierung der sektoralen Zuordnung nicht vorsieht.[15]

Gleichzeitig eröffnet § 28 Abs. 3 BSIG Unternehmen erhebliche Auslegungsspielräume bei der Einordnung ihrer Geschäftstätigkeiten. Ob und in welchem Umfang diese nationale Abweichung unionsrechtlich Bestand haben wird, bleibt letztlich einer Klärung durch den Europäischen Gerichtshof vorbehalten.

c) Zurechnung im Konzern und Ausnahme

Bei der Berechnung dieser Schwellenwerte ist gemäß § 28 Abs. 4 Satz 1 BSIG die Empfehlung der Kommission 2003/361/EG anzuwenden.[16] Vereinfacht ausgedrückt bedeutet dies, dass die maßgeblichen Schwellenwerte in Konzernstrukturen grundsätzlich unter Einbeziehung der Partner- und verbundenen Unternehmen zu ermitteln sind.

Dagegen findet nach § 28 Abs. 4 Satz 2 BSIG keine Zurechnung statt, wenn ein Partner- oder verbundenes Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen oder tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist (siehe auch Erwägungsgrund 16 NIS2-Richtlinie).

Im Zusammenhang mit der Zurechnung im Konzern ist darauf hinzuweisen, dass die *materielle* Betroffenheit nach dem BSIG stets unternehmensscharf zu bestimmen ist. Das Überschreiten der maßgeblichen Schwellenwerte auf Konzernebene führt mit anderen Worten nicht dazu, dass automatisch jedes Konzernunternehmen in den Anwendungsbereich der NIS2-Regelungen fällt. Die materielle Anwendbarkeit bleibt vielmehr stets einrichtungsbezogen und knüpft an die konkrete Tätigkeit des jeweiligen Unternehmens an.

III. Anwendbarkeit der NIS2 auf Zulieferer

Grundsätzlich stellen sich auch für die Zulieferer der OEMs vergleichbare Fragen der Anwendbarkeit der NIS2-

der Kunden oder aus der Ferne" sowie „*ein Managed Service Provider, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt*".

12 https://www.bsi.bund.de/dok/nis-2-sektor-faq (Abruf 31.12.2025).

13 Dazu *Döveling/Hempel*, in: Bernzen/Heinze/Steinrötter, DSRI Herbstakademie 2025, 2025, 287 f. m. w. N.; *Döveling/Hempel* kommen zu dem Ergebnis, dass der „deutsche Sonderweg" europarechtskonform sei. Zunächst war vorgesehen, dass „auf die der Einrichtungsart zuzuordnenden Geschäftstätigkeit" abzustellen sein soll; dazu kritisch *Hessel/Schneider*, MMR 2025, 243, 246.

14 Zur Auslegung auch: https://www.bsi.bund.de/dok/nis-2-faq-allgemein (Abruf: 10.1.2026).

15 Vgl. Stellungnahme des Verbands der Internetwirtschaft zum „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" (NIS-2- Umsetzungs- und Cybersicherheitsstärkungsgesetz) des Bundesministeriums des Innern vom 4.7.2025, S. 7.

16 Siehe dazu auch den Benutzerleitfaden zur Definition von KMU: https://publications.europa.eu/resource/cellar/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1.0004.01/DOC_1 (Abruf: 6.1.2026).

Gesetze wie soeben dargestellt. Die Prüfungslogik der territorialen Anwendbarkeit sowie der Zuständigkeit der nationalen Aufsichtsbehörden ist insoweit analog zu den oben dargestellten Grundsätzen. Wie bereits ausgeführt, erfassen die für OEMs relevanten Sektoren auch solche Tätigkeiten, die typischerweise bei Zulieferern anzutreffen sind. Dies gilt etwa für Hersteller von Kraftwagenmotoren (vgl. Ziffer 29.10 der NACE Rev. 2), elektrischen Ausrüstungsgegenständen wie Lichtmaschinen oder Zündkerzen (vgl. Ziffer 29.31 der NACE Rev. 2) oder Bremsen, Getrieben, Achsen, Rädern, Stoßdämpfern, Sicherheitsgurten, Airbags, Türen und Stoßstangen (vgl. Ziffer 29.32 der NACE Rev. 2).

Im Folgenden wird zunächst die unmittelbare Anwendbarkeit der NIS2-Regelungen auf Zulieferer dargestellt. Daran anschließend wird die mittelbare Betroffenheit von Zulieferern über die Lieferkette beleuchtet.

1. Unmittelbare Anwendbarkeit von NIS2-Gesetzen auf Zulieferer

Zulieferer von OEMs können – unabhängig davon, welchem *Tier* sie zuzuordnen sind – häufig selbst in den Anwendungsbereich der NIS2-Regelungen fallen. Maßgeblich ist auch hier, ob sie einer der in den Anlagen zum BSIG genannten Einrichtungsarten zuzuordnen sind. Ausgehend von der deutschen Umsetzungssystematik kommen für Zulieferer insbesondere die nachfolgenden Einrichtungsarten in Betracht, wobei die Darstellung der Auflistung in Anlage 2 zum BSIG folgt.

a) Mögliche einschlägige Sektoren

Zunächst kann in Betracht kommen, dass ein Zulieferer selbst *Abfallbewirtschaftung* im Sinne von § 3 Abs. 14 Kreislaufwirtschaftsgesetz betreibt (Ziffer 2.1.1 der Anlage 2 zum BSIG). Dabei sind jedoch solche Betriebe und Unternehmen auszunehmen, bei denen die Abfallbewirtschaftung nicht die Hauptwirtschaftstätigkeit darstellt.

Weiterhin ist aus dem Sektor *Produktion, Herstellung und Handel mit chemischen Stoffen*[17] die unter Ziffer 3.1.1 der Anlage 2 zum BSIG genannte Einrichtungsart relevant. In der Praxis werden Zulieferer häufig chemische Stoffe oder Gemische importieren, da diese für den jeweiligen Herstellungsprozess erforderlich sind. Zu beachten ist hierbei, dass der deutsche Gesetzgeber von der Systematik der NIS2-Richtlinie abweicht. Er erfasst lediglich Hersteller und Importeure im Sinne der REACH-Verordnung, nicht jedoch Händler. Eine weitere Einschränkung besteht darin, dass die Stoffe oder Gemische der Abteilung 20 der NACE Rev. 2 zuzuordnen sein müssen und das Unternehmen zugleich der Registrierungspflicht nach Art. 6 der REACH-Verordnung unterliegt.

Für Zulieferer kann ferner die Branche *Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen*[18] einschlägig sein (Ziffer 5.2.1 der Anlage 2 zum BSIG). Die maßgeblichen Unternehmen ergeben sich aus Abschnitt C Abteilung 26 der NACE Rev. 2. Erfasst sind insbesondere Unternehmen, die elektronische Komponenten oder Systeme herstellen, die typischerweise in Fahrzeugen oder fahrzeugnahen Anwendungen eingesetzt werden (z. B. elektronische Bauelemente, Leiterplatten, Sensorik oder bestimmte Steuerungskomponenten). Ob einzelne komplexe Fahrzeugsysteme, etwa Infotainment- oder Assistenzsysteme, vollständig unter diese Abteilung fallen, ist nicht in allen Fällen eindeutig und bedarf einer einzelfallbezogenen Prüfung.

Ebenfalls relevant kann für Zulieferer die Branche *Herstellung von elektrischen Ausrüstungen* sein, die in Ziffer 5.3.1 der Anlage 2 zum BSIG sowie in Abschnitt C Abteilung 27 der NACE Rev. 2 erfasst ist. Darunter fallen Unternehmen, die elektrische Komponenten oder Systeme herstellen, welche für den Fahrzeugbetrieb oder die Energieversorgung wesentlich sind (z. B. Elektromotoren, Batterien oder elektrische Leitungs- und Verteilungssysteme).

Weiterhin kann für Zulieferer die Branche *Maschinenbau* relevant sein. Maßgeblich ist hierbei die Einrichtungsart nach Ziffer 5.4.1 der Anlage 2 zum BSIG in Verbindung mit Abteilung 28 der NACE Rev. 2. Erfasst sind insbesondere Unternehmen, die maschinen- oder antriebstechnische Komponenten herstellen, die typischerweise in Fahrzeugen oder deren Produktionsprozessen eingesetzt werden (z. B. Kolben, Ein- und Auslassventile, hydraulische oder pneumatische Bauteile sowie Lager-, Getriebe- oder Antriebselemente).

Wie bereits für OEMs dargestellt, ist auch für Zulieferer die Branche *Herstellung von Kraftwagen und Kraftwagenteilen* relevant. Nach Abteilung 29 der NACE Rev. 2 umfasst dies insbesondere die Herstellung von Kraftwagenmotoren, Karosserien, Aufbauten und Anhängern sowie die Herstellung von Teilen und Zubehör für Kraftwagen (vgl. insbesondere Abteilung 29.3 der NACE Rev. 2). Gerade Zulieferer, deren Tätigkeit schwerpunktmäßig auf der Entwicklung oder Fertigung solcher Komponenten liegt, können damit unmittelbar in den Anwendungsbereich der NIS2-Regelungen fallen.

b) (Fehlende) Definition des Herstellens

Wie soeben gezeigt, ist vor allem das „Herstellen“[19] von besonderer Relevanz. Gleichzeitig enthält weder das BSIG noch die NIS2-Richtlinie eine Definition des Begriffs des Herstellens. Auch die NACE Rev. 2 enthält insoweit keine eigenständige Legaldefinition. Vor diesem Hintergrund spricht viel dafür, den Begriff eng auszulegen und auf das rein faktische Herstellen abzustellen. Danach sind grundsätzlich nur solche Unternehmen als Hersteller anzusehen, die den eigentlichen Herstellungsprozess tatsächlich selbst durchführen. Wird der Herstellungsprozess ausgelagert, fehlt es regelmäßig an einer eigenen Herstellungstätigkeit, sodass die entsprechenden Regelungen des BSIG und der NIS2-Richtlinie nicht einschlägig sind.[20]

---

17 Siehe dazu auch: *Nink*, Das neue IT-Sicherheitsrecht, 2026, § 2 Rn. 47 f.

18 Zum Verarbeitenden Gewerbe/Herstellung von Waren: *Nink*, ZfPC 2025, 58; *Woronka*, unternehmensjurist 2024, 26.

19 Hierzu auch *Hessel/Schneider*, MMR 2025, 243, 245.

20 Vgl. hierzu jedoch auch Rn. 83 der NACE Rev. 2 zur Auslagerung von Herstellungstätigkeiten. Die dort angesprochene Zuordnung eines Auftraggebers zum verarbeitenden Gewerbe knüpft insbesondere an Eigentum an Input-Rohstoffen und Output an; eine zwingende Gleichsetzung mit einer Herstellerrolle im Sinne der sektoralen Zuordnung nach Abschnitt C NACE Rev. 2 lässt sich daraus jedoch nicht eindeutig ableiten.

2. Mittelbare „Betroffenheit" über die Lieferkette

Auch wenn – wie gezeigt – die Kriterien für eine unmittelbare Anwendbarkeit der NIS2-Regelungen sehr weit gefasst sind, kommt es in Betracht, dass einzelne Zulieferer nicht selbst in den Anwendungsbereich der NIS2 fallen.

Unabhängig davon sind OEMs seit jeher bestrebt, Informationssicherheitsvorgaben entlang der gesamten Lieferkette durchzusetzen. Dies hat unter anderem zur Entwicklung von TISAX als branchenspezifischem Standard geführt. Darüber hinaus enthalten auch die Allgemeinen Einkaufsbedingungen der OEMs regelmäßig konkrete Vorgaben dazu. Vor diesem Hintergrund ist davon auszugehen, dass OEMs, die selbst in den Anwendungsbereich der NIS2-Regelungen fallen, auch künftig innerhalb ihrer Lieferketten entsprechende Sicherheitsmaßnahmen von ihren Zulieferern verlangen werden, selbst wenn diese nicht unmittelbar als Einrichtung im Sinne der NIS2-Richtlinie erfasst sind.

OEMs sind gemäß § 30 Abs. 2 Nr. 4 BSIG verpflichtet, Maßnahmen zur Herstellung und Absicherung der Lieferkettensicherheit zu ergreifen. Vor diesem Hintergrund werden sie selbst ein erhebliches Interesse daran haben, wie ihre Zulieferer Cyberrisiken adressieren und ihre Cyberverantwortung organisatorisch verankern. In der Praxis erfolgt dies regelmäßig über vertragliche Vorgaben. Dazu zählen insbesondere Verpflichtungen zur Implementierung eines Informationssicherheitsmanagementsystems sowie zu entsprechenden Nachweisen, etwa durch Zertifizierungen nach TISAX oder ISO/IEC 27001.

IV. Materielle Pflichten des BSIG

1. Überblick über die 10-Punkte-Liste nach § 30 BSIG

Eines der Kernelemente der NIS2-Regelungen sind die von wichtigen und besonders wichtigen Einrichtungen zu ergreifenden Risikomanagementmaßnahmen.[21] Diese ergeben sich in der deutschen Umsetzung aus § 30 BSIG und entsprechen inhaltlich den Vorgaben des Art. 21 NIS2-Richtlinie.

Zentraler Ausgangspunkt der Risikomanagementmaßnahmen ist eine Risikoanalyse gemäß § 30 Abs. 1 BSIG.[22] Die Risikoanalyse bildet die Grundlage für alle weiteren Maßnahmen und hat sich an den spezifischen Risiken der jeweiligen Einrichtung, ihrer Tätigkeiten sowie ihrer Einbindung in Liefer- und Wertschöpfungsketten zu orientieren.

Auf Basis der Risikoanalyse sind sodann die in § 30 Abs. 2 Satz 2 BSIG genannten Maßnahmen umzusetzen. Der Gesetzgeber nennt insoweit einen Katalog von zehn Maßnahmen, deren konkrete Ausgestaltung dem jeweiligen Unternehmen obliegt. Dabei ist der Stand der Technik[23] einzuhalten.

Der Maßnahmenkatalog des § 30 Abs. 2 Satz 2 BSIG ist breit angelegt. Er umfasst unter anderem Konzepte zur Sicherheit in der Informationstechnik (Nr. 1), Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs (Nr. 3), Vorgaben zur Sicherheit der Lieferkette (Nr. 4), Sicherheitsanforderungen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen und Komponenten (Nr. 5) sowie Schulungen für alle Mitarbeitenden (Nr. 7).

Auf Grundlage von Art. 21 Abs. 5 NIS2-Richtlinie (vgl. auch § 30 Abs. 3, 4 und 5 BSIG) hat die Europäische Kommission für bestimmte digitale Dienste Durchführungsrechtsakte erlassen. Diese sind für die jeweils erfassten Einrichtungsarten vorrangig anzuwenden. Sie gelten ausschließlich für die dort genannten Unternehmen, können jedoch auch von anderen Einrichtungen als Orientierungspunkt für die Ausgestaltung ihrer Risikomanagementmaßnahmen herangezogen werden.

Der deutsche Gesetzgeber hat in den Gesetzgebungsmaterialien ausdrücklich klargestellt, dass die Risikomanagementmaßnahmen nicht lediglich für einzelne, besonders kritische informationstechnische Systeme oder sogenannte „NIS2-Assets" umzusetzen sind. Vielmehr sind die Maßnahmen unternehmensweit auszurollen und auf die gesamte Organisation – und damit sowohl IT als auch OT – zu beziehen.[24]

a) Cybersicherheit in der Lieferkette

Für die Automotive-Branche besonders hervorzuheben ist die Verpflichtung zu angemessenen Sicherheitsmaßnahmen für die Lieferkette gemäß § 30 Abs. 2 Satz 2 Nr. 4 BSIG.[25] Diese Pflicht gewinnt im industriellen Umfeld der Automobilwirtschaft besondere Bedeutung, da OEMs aufgrund ihrer Marktmacht seit jeher einen starken Fokus auf die vertragliche Ausgestaltung von Informationssicherheitsanforderungen entlang der Lieferkette legen.

In der Praxis enthalten die Allgemeinen Einkaufsbedingungen der OEMs bereits heute vielfach weitreichende und teilweise abstrakt formulierte Verpflichtungen. Zulieferer werden regelmäßig zur Implementierung eines angemessenen Informationssicherheitsmanagementsystems sowie zu geeigneten organisatorischen Maßnahmen verpflichtet. Weder die NIS2-Richtlinie noch das BSIG enthalten jedoch konkrete Vorgaben dazu, wie die Lieferkette im Einzelnen abzusichern ist. Das BSI betont insoweit, dass es keine „One-Size-Fits-All-Lösung" gibt.

Vielmehr haben die Unternehmen risikobasiert zu bestimmen, wie sie ihre Lieferkette absichern wollen. Dies erfolgt regelmäßig durch die Festlegung interner Leitlinien, aus denen konkrete Maßnahmen abgeleitet werden. Erwartbar ist dabei eine Kombination aus strukturierten Abfragen bei Zulieferern, vertraglichen Verpflichtungen zur Umsetzung bestimmter Sicherheitsmaßnahmen (etwa in Anlehnung an bekannte Kataloge technischer und organisatorischer Maßnahmen) sowie der Vereinbarung von Audit- und Kontrollrechten, um die Einhaltung der Vorgaben überprüfbar zu machen.

Da – wie gezeigt – viele Zulieferer ihrerseits unmittelbar in den Anwendungsbereich der NIS2-Regelungen bezie-

21 Dazu allgemein *Döveling/Hempel*, in Bernzen/Heinze/Steinrötter, DSRI Herbstakademie 2025, 2025, 292 ff.; *Nink*, ZfPC 2025, 58, 64 f.; *Heinelt/Dittrich/Basar*, CB 2025, 151, 153 f.

22 Siehe dazu die Infoseite des BSI: https://www.bsi.bund.de/dok/nis-2-risikoanalyse (Abruf: 6.1.2026).

23 Siehe dazu etwa TeleTrusT, Handreichung Stand der Technik in der IT-Sicherheit, https://www.teletrust.de/publikationen/broschueren/stand-der-technik/ (Abruf: 6.1.2026); siehe auch: https://www.bsi.bund.de/dok/Stand-der-Technik (Abruf 10.1.2026).

24 BT-Drucks. 21/1501, S. 147.

25 Siehe dazu die Infoseite des BSI: https://www.bsi.bund.de/dok/nis-2-sichere-lieferkette (Abruf: 6.1.2026); ausführlich hierzu auch *Blum/Adelberg*, CB 2024, 461.

hungsweise des BSIG fallen dürften, ist zugleich zu erwarten, dass diese die entsprechenden Anforderungen wiederum entlang ihrer eigenen Lieferketten weiterreichen.

b) Verhältnis zu bestehenden Standards und Frameworks
Für Unternehmen der Automotive-Branche stellt sich in diesem Zusammenhang regelmäßig die Frage, inwieweit bereits etablierte Standards und Frameworks die Anforderungen des § 30 Abs. 2 BSIG abbilden. In der Praxis greifen viele Unternehmen auf bestehende Rahmenwerke zurück, etwa auf TISAX als branchenspezifischen Standard der Automobilindustrie,[26] auf ein Informationssicherheitsmanagementsystem nach ISO/IEC 27001, auf branchenspezifische technische Regelwerke wie die VdS-Richtlinien 10000[27] oder auf ein Cybersecurity Management System nach der UN-Regelung Nr. 155. Diese Standards und Frameworks adressieren jeweils zentrale Elemente der Informationssicherheit und des Risikomanagements und können daher als Ausgangspunkt für die Umsetzung der gesetzlichen Anforderungen dienen.

Dabei kann jedoch nicht pauschal davon ausgegangen werden, dass die bloße Erfüllung der genannten Standards oder Frameworks sämtliche Anforderungen des § 30 BSIG unmittelbar erfüllt. Unternehmen, die solche Standards implementiert haben, dürften jedoch regelmäßig nur noch begrenzte Abweichungen zu den regulatorischen Vorgaben aufweisen und auf einer belastbaren Ausgangsbasis aufsetzen können.

c) Nachweispflichten und Dokumentation
Hinsichtlich der Dokumentation sieht § 30 Abs. 1 Satz 3 BSIG vor, dass die Einrichtungen die Erfüllung ihrer Verpflichtungen nach Satz 1 zu dokumentieren haben. Dieser *Accountability*-Grundsatz, der auch aus Art. 5 Abs. 2 DSGVO bekannt ist, führt dazu, dass Unternehmen nicht nur die ergriffenen Maßnahmen, sondern auch die Durchführung der Risikoanalyse sowie die daraus abgeleiteten Maßnahmen oder bewussten Risikoakzeptanzen nachvollziehbar dokumentieren müssen. Das BSI hat bei besonders wichtigen Einrichtungen das Recht, (verdachtsunabhängig) entsprechende Nachweise zu verlangen (§ 61 Abs. 3 BSIG); bei wichtigen Einrichtungen besteht eine verdachtsabhängige Überprüfungsmöglichkeit (§ 62 BSIG).

2. Weitere Pflichten (insbesondere Registrierung, Schulungen und Meldepflichten)

Das BSIG enthält neben den dargestellten Risikomanagementmaßnahmen weitere Verpflichtungen für wichtige und besonders wichtige Einrichtungen. Auf diese wird im vorliegenden Aufsatz nicht vertieft eingegangen, da sie keine spezifischen Besonderheiten für die Automotive-Branche aufweisen.

Die betroffenen Einrichtungen müssen sich bei der zuständigen Behörde, in Deutschland dem BSI, registrieren, § 33 BSIG. Darüber hinaus sieht das BSIG besondere Pflichten für die Geschäftsleitung vor. Danach haben sich die Mitglieder der Geschäftsleitung im Sinne von § 2 Nr. 13 BSIG gemäß § 38 Abs. 3 BSIG regelmäßig zu Fragen der Cybersicherheit und des Risikomanagements schulen zu lassen.[28]

Gemäß § 32 BSIG haben wichtige und besonders wichtige Einrichtungen erhebliche Cybersicherheitsvorfälle unverzüglich an das BSI zu melden.[29] Von besonderer praktischer Relevanz ist dabei, dass eine Erstmeldung binnen 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall abzugeben ist. Diese frühe Meldung dient der schnellen Lageeinschätzung und erfolgt regelmäßig, bevor der Sachverhalt vollständig aufgeklärt ist.

Darüber hinaus ist spätestens binnen 72 Stunden eine erste Folgemeldung einzureichen. Ein Abschlussbericht ist sodann spätestens innerhalb eines Monats nach dem erheblichen Sicherheitsvorfall zu übermitteln. Die näheren Einzelheiten zur Ausgestaltung des Meldeverfahrens werden vom BSI gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe noch konkretisiert (§ 32 Abs. 4 BSIG).

Die Meldepflichten werfen derzeit noch verschiedene offene Rechtsfragen auf. So ist bislang nicht eindeutig geklärt, ob sich erhebliche Cybersicherheitsvorfälle ausschließlich auf solche informationstechnischen Systeme und Prozesse beziehen, die für die jeweilige Einrichtungsart maßgeblich sind. Es ist jedoch naheliegender, dass alle Vorfälle im Rahmen des BSIG gemeldet werden müssen.

In der Praxis aufwendig ist der Umgang mit Meldepflichten in (internationalen) Konzernstrukturen. Bei grenzüberschreitenden Vorfällen werden die Einrichtungen Vorfälle parallel an mehrere nationale Behörden melden müssen. Dies führt zu zusätzlichen praktischen Herausforderungen, unter anderem im Hinblick auf betriebsverfassungsrechtliche und arbeitsrechtliche Fragestellungen. Die 24-stündige Meldefrist setzt voraus, dass Unternehmen eine entsprechende organisatorische und personelle Infrastruktur vorhalten, etwa durch Bereitschaftsmodelle oder vergleichbare organisatorische Vorkehrungen.

V. (Management-)Verantwortung und Umsetzung – auch in Konzernstrukturen

Bei einer Verletzung der Pflichten nach dem neuen BSIG drohen empfindliche Konsequenzen – und zwar nicht nur für das betroffene Unternehmen selbst (etwa in Form von empfindlichen Bußgeldern in Höhe von bis zu 10 Mio. Euro, vgl. § 65 Abs. 5 Nr. 1 lit. a) BSIG), sondern auch für dessen Vorstand. Nach § 38 Abs. 1 BSIG haben die „*Geschäftsleitungen*“ die oben erwähnten Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen. Das Gesetz adressiert in diesem Zusammenhang jede natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist (vgl. § 2 Nr. 13 BSIG). Soweit die Verantwortlichen dieser Pflicht nicht nachkommen, haften sie gegenüber ihrem Unternehmen für den daraus entstandenen Schaden.

26 Siehe dazu das ausführliche Mapping der ENX Association: https://enx.com/de-de/news/TISAX-NIS2/ (Abruf: 6.1.2026).
27 Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU).
28 Siehe dazu die Infoseite des BSI: https://www.bsi.bund.de/dok/nis-2-schulung-geschaeftsleitung (Abruf: 6.1.2026); siehe auch *Teichmann*, CR 2025, 718.
29 Siehe dazu die Infoseite des BSI: https://www.bsi.bund.de/dok/nis-2-meldepflicht (Abruf: 6.1.2026); siehe auch *Grosmann/Michel*, ZD 2025, 250, 253.

Diese persönliche Haftung wirft unmittelbar die Frage nach Inhalt, Reichweite und Adressaten der Verantwortlichkeit auf Vorstandsebene auf. Der Gesetzgeber knüpft – in Umsetzung von Art. 20 NIS2-Richtlinie – nicht an formale Organbezeichnungen, sondern an eine funktionale Leitungsverantwortung an. Maßgeblich ist, wer tatsächlich die unternehmerischen Leitungs- und Organisationsentscheidungen trifft und hierfür rechtlich verantwortlich ist.

Diese funktionale Betrachtungsweise erlaubt zugleich die Anwendung auf unterschiedliche Governance-Modelle. In dualistischen Leitungssystemen, wie sie etwa das deutsche Aktienrecht mit der Trennung von Vorstand und Aufsichtsrat vorsieht,[30] ist der Vorstand Träger der originären Leitungs- und Organisationsverantwortung, während dem Aufsichtsrat lediglich eine Überwachungsfunktion zukommt. Die Pflichten aus § 38 BSIG treffen daher den Gesamtvorstand als Kollegialorgan; eine Ressortverteilung vermag lediglich den internen Haftungsmaßstab zu modifizieren, nicht aber die gesetzlich angeordnete Gesamtverantwortung aufzuheben.[31] Demgegenüber sind in monistischen Systemen – etwa im Vereinigten Königreich oder in Frankreich – die Leitungs- und Überwachungsfunktionen im Board of Directors[32] bzw. Conseil d'administration[33] zusammengeführt, sodass sämtliche Executive Directors als Geschäftsleiter im Sinne des BSIG anzusehen sind.

Besondere praktische Relevanz entfaltet dies im Konzernkontext. Zwar adressiert das BSIG – ebenso wie die NIS2-Richtlinie – grundsätzlich die einzelne juristische Person; gleichwohl erzwingen zentralisierte IT-Infrastrukturen, konzernweite Sicherheitsarchitekturen und einheitliche Incident-Response-Strukturen eine faktische Verantwortungskonzentration auf oberster Ebene. Eine vollständige Verlagerung der Verantwortung auf Tochtergesellschaften ist mit § 38 BSIG nicht vereinbar. Zulässig ist lediglich eine operative Delegation, die von klaren Governance-Strukturen, belastbaren Berichtslinien und einer effektiven Überwachung flankiert wird.

Damit verbunden sind erhebliche Haftungs- und Organisationsfragen. Der Vorstand schuldet nicht die Verhinderung jedes Cybervorfalls, wohl aber die Einrichtung eines angemessenen, risikoorientierten Organisations- und Kontrollsystems. Maßstab sind hierbei die bekannten Grundsätze der ordnungsgemäßen Unternehmensorganisation, wie sie bereits aus § 93 Abs. 1 AktG bzw. § 43 Abs. 1 GmbHG folgen. Defizite bei der Risikoanalyse, fehlende Berichtswege oder eine lediglich formale Delegation können als Organisationsverschulden haftungsrelevant werden.[34]

Inhaltlich umfasst die Verantwortung der Geschäftsleitung insbesondere die Billigung der Risikomanagementmaßnahmen, deren fortlaufende Überwachung sowie – als neue und besonders hervorgehobene Pflicht – die regelmäßige Teilnahme an Schulungen. Diese Schulungspflicht dient nicht der technischen Detailqualifikation, sondern soll die Geschäftsleiter in die Lage versetzen, Cyberrisiken zu erkennen, Maßnahmen zu bewerten und deren Auswirkungen auf die Geschäftstätigkeit einzuordnen.[35]

Für die Praxis von Vorstand und Geschäftsführung folgt daraus, dass Cybersicherheit und Informationssicherheitsmanagement als originäre Leitungsaufgaben zu begreifen sind. Erforderlich sind belastbare Governance-Strukturen, dokumentierte Entscheidungsprozesse, regelmäßige Risikoanalysen sowie eine fortlaufende Berichterstattung an die Leitungsebene. Zugleich gewinnt die D&O-Versicherung an Bedeutung, wobei zu beachten ist, dass sie zwar das finanzielle Haftungsrisiko abfedern kann, jedoch eine ordnungsgemäße Organisation nicht ersetzt. Insgesamt verschärft das BSIG damit die Anforderungen an die persönliche Verantwortung der Unternehmensleitung und verankert Cybersicherheit als zentralen Bestandteil moderner Corporate Governance.

VI. Fazit

1. *Die materiellen Pflichten des BSIG und der NIS2-Richtlinie sind für die Automotive-Branche weitgehend erwartbar*: Angesichts der bereits heute hohen Anforderungen an die Informationssicherheit verfügen viele OEMs und Zulieferer über eine belastbare Vorarbeit. Der zusätzliche Umsetzungsaufwand dürfte sich daher in der Praxis häufig in überschaubaren Grenzen halten.
2. *Die Anwendbarkeit des BSIG ist im Automotive-Sektor der Regelfall*: Sowohl OEMs als auch ein erheblicher Teil der Zulieferer werden aufgrund der sektoralen Zuordnung und der niedrigen Schwellenwerte der Size-Cap-Rule in den Anwendungsbereich fallen. Fälle der Nicht-Anwendbarkeit werden die Ausnahme bleiben und bedürfen einer sorgfältigen Begründung.
3. *Die Pflichten nach dem BSIG sind konsequent unternehmensscharf ausgestaltet, bilden aber die Realität von Konzernen nicht ab*: Diese Systematik entspricht der Logik der NIS2-Richtlinie, bildet jedoch die organisatorischen und operativen Realitäten großer Konzernstrukturen nur unzureichend ab. Dies betrifft insbesondere die territoriale Anwendbarkeit, die Zuständigkeitsordnung der Aufsichtsbehörden sowie die Ausgestaltung der Meldepflichten nach § 32 BSIG. Für konzernweite Vorfälle bestehen bislang keine praxistauglichen, konsistenten Lösungsmodelle, sodass ein frühzeitiger Dialog mit den Aufsichtsbehörden an Bedeutung gewinnt.
4. *Bestehende Standards und Frameworks bieten eine tragfähige, aber keine abschließende Grundlage für die Umsetzung*: Zertifizierungen und Managementsysteme wie TISAX oder ISO/IEC 27001 ersetzen die gesetzlichen Anforderungen nicht, können den Umsetzungsaufwand jedoch deutlich reduzieren und als strukturierender Ausgangspunkt dienen.
5. *Große praktischen Herausforderungen der NIS2-Richtlinie liegen auch in der organisatorischen Verankerung*: Kurze Meldefristen, unternehmensweite Risikomanagementpflichten und kontinuierliche Überwachung erfordern klare Zuständigkeiten, belastbare Entscheidungsprozesse und eine dauerhafte personelle Absicherung. Dies wirft nicht zuletzt arbeits- und betriebsverfassungsrechtliche Fragen auf, etwa im Hinblick auf Bereitschaftsmodelle, Eskalationswege und Verantwortlichkeiten.

30 *Eberspächer*, in BeckOGK, 1.2.2024, SE-VO Art. 38 Rn. 4.
31 *Kipker/Dittrich*, CB 2024, 18 (19 f.).
32 *Heppe*, in Melot de Beauregard/Lieder/Liersch: Managerhaftung-HdB, 1. Aufl. 2022, § 11 Rn. 83.
33 *Opitz*, in Wegen/Spahlinger/Barth, GesR Ausland, Luxemburg Rn. 66.
34 *Blum/Adelberg*, CB 2024, 145, 149 f.; *Teichmann*, CCZ 2025, 265, 271 f.
35 *Teichmann*, CCZ 2025, 265, 266 f.; *Kipker/Dittrich*, CB 2024, 18, 20.