www.betriebs-berater.de

Betriebs Berater

BB

7|2026

Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ...

9.2.2026 | 81. Jg.
Seiten 321–384

80 Jahre

DIE ERSTE SEITE

Prof. Dr. Thorsten Sellhorn und **Prof. Dr. Maximilian Müller**
Warum „Connectivity" jetzt zum Prüfstein moderner Unternehmensberichterstattung wird

WIRTSCHAFTSRECHT

Dr. Kristina Schreiber, RAin
Das neue BSIG 2025 bringt neue Cybersicherheitspflichten für unzählige Branchen: NIS-2-Richtlinie jetzt auch in Deutschland umgesetzt | 323

Marvin Schäfer
Kapitalaufbringungsgrundsatz im Lichte von Online-Zahlungsdienstleistungen, E-Geld und Kryptowährungen | 329

STEUERRECHT

Prof. Dr. iur. Christoph Schmidt
Der NKR-Jahresbericht 2025 und das Steuerrecht: Abbauziele, Digitalcheck und Evaluationskultur im Zusammenspiel – Teil II | 343

BILANZRECHT UND BETRIEBSWIRTSCHAFT

Dr. Florian Kleinmanns, StB/RA/FAStR
Neuere Entwicklungen in Gesetzgebung, Rechtsprechung und Verwaltung bei der Abschreibung von Immobilien | 363

ARBEITSRECHT

Bruno Glöckner, RA/Syndikus-RA
Wahlrecht von Führungskräften in mehreren Betrieben bei unternehmensinterner Matrix-Struktur? Praxistipps anlässlich der Betriebsratswahlen 2026 | 372

BB-Jahresregister 2025

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Dr. Kristina Schreiber, RAin

Das neue BSIG 2025 bringt neue Cybersicherheitspflichten für unzählige Branchen: NIS-2-Richtlinie jetzt auch in Deutschland umgesetzt

Zum 6.12.2025 ist das neue Informationssicherheitsrecht der NIS-2-Richtlinie auch in Deutschland in Kraft getreten, mit über einem Jahr Verspätung. Die NIS-2-Richtlinie hätte schon bis zum 17.10.2024 in nationales Recht umgesetzt werden müssen, Deutschland hatte dies insbesondere aufgrund der Neuwahlen im Frühjahr 2025 nicht realisieren können. Das am 5.12.2025 verkündete Gesetz zur Umsetzung der NIS-2-Richtlinie enthält in seinem Art. 1 mit der Neufassung des BSIG nunmehr aber das Herzstück der neuen Pflichten für rund 30 000 Unternehmen, die diese ohne Übergangsfrist einzuhalten haben. Für welche Einrichtungen ab wann welche Pflichten gelten, zeigt dieser Beitrag auf.

I. Verschärfung des Informationssicherheitsrechts

Digitale Innovationen sind nicht erst seit dem Vormarsch von Anwendungen künstlicher Intelligenz (KI) allgegenwärtig: Die digitale Transformation ist in vollem Gange. Mit der zunehmenden Digitalisierung wachsen indes auch die Sicherheitsbedürfnisse und Angriffsflächen im digitalen Raum.[1] Dies gilt umso mehr, als die Cybersicherheit seit Jahren bedroht ist: Etwa der BSI-Lagebericht 2025 zur IT-Sicherheit in Deutschland zeigt erneut eine besorgniserregende Bedrohungslage auf.[2]

Angesichts dieser wachsenden Verwundbarkeit durch die digitale Transformation einerseits und eine steigende Bedrohungslage andererseits hat sich die EU im Rahmen ihrer Cybersicherheitsstrategie zu einer Verschärfung der Vorgaben des Informationssicherheitsrechts entschieden. Nachdem die Cybersicherheit in der Vergangenheit vor allem als reaktives Handlungsfeld betrachtet wurde, steht nunmehr die Prävention deutlich im Vordergrund. Dies zeigt sich auch in der 2020 veröffentlichte EU-Cybersicherheitsstrategie,[3] die die NIS-2-Richtlinie[4] als wesentlichen Baustein umfasst.

Die NIS-2-Richtlinie verpflichtet alle Unternehmen innerhalb ihres Anwendungsbereichs zu umfassenden Cybersicherheitsmaßnahmen und bildet mit diesen fundamentalen Pflichten das Herzstück der EU-Cybersicherheitsarchitektur. Als EU-Richtlinie muss sie in nationales Recht umgesetzt werden; gem. Art. 41 Abs. 1 NIS-2-Richtlinie hätte das bis zum 17.10.2024 geschehen müssen. Am 20.1.2026 hat die EU-Kommission mit ihrem Vorschlag COM(2026) 13 final bereits Änderungen an der NIS-2-Richtlinie vorschlagen, als Teil des Cybersicherheitspakets 2. Insbesondere sollen die Schwellen für besonders wichtige Einrichtungen angehoben werden (750 Mitarbeitende oder 150 Mio. Euro Jahresumsatz und 129 Mio. Euro Jahresbilanzsumme). Zudem sind eine Reihe von Anpassungen für DNS-Anbieter, digitale Brieftaschen und einzelne weitere Sektoren vorgesehen sowie die Einführung eines Zertifikats, mit dem die NIS-2-Compliance nachgewiesen werden kann. Diese Vorschläge müssen indes noch das EU-Gesetzgebungsverfahren durchlaufen.

1. Evolution von NIS-1 zu NIS-2: Lektionen aus der Praxis

Die NIS-2-Richtlinie unterscheidet sich hinsichtlich des Anwendungsbereichs in zwei zentralen Punkten von ihrer Vorgängerin, der ersten NIS-Richtlinie:[5]

- Der Anwendungsbereich beider Richtlinien richtet sich nach dem Sektor, in dem die jeweilige Einrichtung tätig ist, sowie nach bestimmten Schwellenwerten, die die Einrichtung überschreiten muss, um erfasst zu werden. Während die erste NIS-Richtlinie ausschließlich Einrichtungen erfasste, die der Grundversorgung dienen und damit Teil der kritischen Infrastruktur sind, adressiert die NIS-2-Richtlinie deutlich mehr Sektoren. Etwa in Deutschland geht der Gesetzgeber davon aus, dass gegenüber den bisher rund 1 200 registrierten KRITIS-Anlagenbetreibern[6] nunmehr rund 30 000 Einrichtungen reguliert sind.[7]
- Zudem überließ die erste NIS-Richtlinie es den Mitgliedstaaten, wie die Schwellenwerte zu bestimmen sind, damit ein Unternehmen in den Anwendungsbereich der Richtlinie fällt.[8] Diese Schwellenwertberechnungen richteten sich insbesondere danach, welche Bedeutung eine Einrichtung für die Grundversorgung des jeweiligen Mitgliedstaates hat.[9] In Deutschland ist dies maßgeblich durch die BSI-KritisV geschehen. Andere EU-Mitgliedstaaten haben sich für abweichende Schwellen entschieden.Mit der NIS-2-Richtlinie wurde dieses System grundlegend neu strukturiert. Die relevanten Schwellenwerte sind in der Richtlinie selbst angegeben und führen so zu einem einheitlicheren Cybersicherheitsniveau innerhalb der Union; Spielraum nach unten verbleibt den Mitgliedstaaten nicht, wobei eine strengere und damit auch mit Blick auf die Adressaten umfassendere nationale Regulierung möglich wäre (Mindestharmonisie-

1 S. dazu nur *Schreiber/Fischbach*, Die NIS-2-Richtlinie in der EU-Digitalstrategie: Cybersecurity als Fundament für digitalen Wohlstand, MMR-Beilage 2026, im Erscheinen.
2 BSI, Die Lage der IT-Sicherheit in Deutschland, 2025, unter https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html (Abruf: 23.1.2026).
3 Gemeinsame Mitteilung an das Europäische Parlament und den Rat, JOIN(2020) 18 final, Die Cybersicherheitsstrategie der EU für die digitale Dekade, II. 1.
4 RL (EU) 2022/2555.
5 RL (EU) 2016/1148.
6 S. dazu „KRITIS in Zahlen", unter https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html (Abruf: 23.1.2026).
7 BT-Drs. 21/1501, 188.
8 Art. 5 Abs. 1 RL (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194, S. 1–30).
9 Art. 5 Abs. 7 lit. d RL (EU) 2016/1148.

rung). Adressiert werden einige Branchen größenunabhängig und im Übrigen bereits kleine Unternehmen ab 50 Mitarbeitenden oder 10 Mio. Euro Jahresumsatz und Jahresbilanzsumme.[10]

Maßgeblicher Grund für diese Weiterentwicklung waren die durch die Kommission identifizierten Schwachstellen der ersten NIS-Richtlinie sowie der sich über die Jahre deutlich verschärften Bedrohungslage: Die unzureichende Harmonisierung zwischen den Mitgliedstaaten aufgrund unterschiedlicher Umsetzungen führte zu erheblich divergierenden Sicherheitsniveaus. Der Regelungsansatz der NIS-2-Richtlinie ist damit – entsprechend der veränderten Bedrohungslage – deutlich breiter und umfassender.[11]

2. Zentrale Neuerungen der NIS-2-Richtlinie

Neben dem breiteren und präziser definierten Anwendungsbereich führt die NIS-2-Richtlinie zu zahlreichen weiteren Änderungen. Einrichtungen, die in den Anwendungsbereich der Richtlinie fallen, müssen sich registrieren, erhebliche Sicherheitsvorfälle melden und sind zu umfassenden Risikomanagementmaßnahmen verpflichtet, die hinsichtlich der Risikoexposition, der Größe der Einrichtung, der Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere verhältnismäßig erscheinen müssen.[12] Die ergriffenen Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen und sich auf sämtliche Informationstechnischen Systeme, Komponenten und Prozesse beziehen, die von der Einrichtung genutzt werden, um ihre Dienstleistungen zu erbringen. Damit sind auch Lieferketten inbegriffen. Auf gesetzgeberischer Ebene sind diese Verpflichtungen neu, lehnen sich jedoch inhaltlich an den etablierten IT-Grundschutz des BSI und den ISO27001-Standard an.[13] Zudem wird die Letztverantwortung der Leitungsorgane ausdrücklich festgehalten. Diese werden zudem zu regelmäßigen Schulungen verpflichtet.[14]

3. Umsetzung in Deutschland

Am 5.12.2025 wurde das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG) im Bundesgesetzblatt[15] verkündet. Nach Art. 30 NIS2UmsuCG ist das Gesetz am Tag nach seiner Verkündung, also am 6.12.2025, in Kraft getreten. Übergangsfristen gibt es nicht.

Als Artikelgesetz bringt das NIS2UmsuCG Neuerungen für eine Vielzahl an Gesetzen. Im Zentrum steht die Neufassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz, kurz: BSIG) in Art. 1 NIS2UmsuCG. Das BSIG ist das Fundament der symmetrischen Informationssicherheitspflichten in Deutschland. Art. 2 ff. NIS2UmsuCG ändern – asymmetrisch – eine Reihe an sektorspezifischen Gesetzen, vom Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz über das Atomgesetz bis hin zum SGB V.

Das NIS2UmsuCG setzt die NIS-2-Richtlinie mit einiger Verspätung um. Die Umsetzung der NIS-2-Richtlinie im BSIG erhöht nicht nur die Cybersicherheitsanforderungen für die Bundesverwaltung, sondern erweitert insbesondere den Kreis der von dem Gesetz betroffenen Privatunternehmen erheblich, sodass nunmehr nicht mehr nur KRITIS-Betreiber von den Cybersicherheitspflichten betroffen sind.

Mit der nunmehr erfolgten Umsetzung ist auch das von der Kommission wegen der Verzögerung bereits im November 2024 eingeleitete EU-Vertragsverletzungsverfahren gegenstandslos geworden. Deutschland konnte so die Einreichung einer Vertragsverletzungsklage vor dem EuGH nach Art. 258 Abs. 2 AEUV noch verhindern.

Seit Inkrafttreten des neuen BSIG entfalten die Regelungen auch in Deutschland unmittelbare Wirkung gegenüber den Adressaten. Das war mangels unmittelbarer Wirkung der NIS-2-Richtlinie zuvor noch nicht der Fall. Zuständig für den Vollzug ist das Bundesamt für die Sicherheit in der Informationstechnik, kurz BSI.

Das BSIG verfolgt das Ziel, die Sicherheit von IT-Systemen und digitalen Infrastrukturen in Deutschland zu stärken. Es soll vor allem verhindern, dass Informationssysteme durch Cyberangriffe beschädigt, ausspioniert oder außer Betrieb gesetzt werden und hierdurch Gefahren und Schäden für Wirtschaft und Allgemeinheit entstehen. Es verpflichtet zu diesem Zweck Einrichtungen – Unternehmen und die Bundesverwaltung – insbesondere dazu, sich zu registrieren, bestimmte Mindeststandards zur IT-Sicherheit einzuhalten, auf Leitungsebene die Letztverantwortung zu übernehmen und Sicherheitsvorfälle an das BSI zu melden.

II. Adressierte Einrichtungen

In Umsetzung der NIS-2-Richtlinie adressiert das BSIG seit dem 6.12.2025 deutlich mehr Unternehmen und Einrichtungen als noch zuvor. Die Regulierung ist nicht mehr beschränkt auf die kritische Infrastruktur, die für eine gesellschaftliche Grundversorgung unabdingbar ist. Vielmehr erweitert die NIS-2-Richtlinie und damit auch das BSIG die Regulierung im Gießkannenprinzip auf eine Vielzahl von Unternehmen. Diese sind nicht in jedem Fall gesellschaftskritisch, sondern der Ansatz geht vielmehr über die Anhebung der Informationssicherheit bei einer kritischen Masse an Unternehmen, um so insgesamt, flächendeckend, einen erhöhten Sicherheitsstandard zu erreichen und vergleichbar dem Brandschutz Angriffe jedenfalls in ihrer Flächenwirkung erheblich zu begrenzen.

Dies führt dazu, dass vielfach Unternehmen adressiert sind, die sich selbst nicht als „kritisch" für die Gesellschaft einstufen, so etwa auch Uhrmacher, die Hersteller von Lichterketten oder die Konzern-IT-Töchter, die nur die mit ihnen verbundenen Unternehmen mit IT-Dienstleistungen versorgen.

Betroffen sind Einrichtungen als wichtige Einrichtungen oder besonders wichtige Einrichtungen, unter denen auch die KRITIS-Betreiber mit weiterhin verschärften Anforderungen sind.

1. Relevante Sektoren

Zu welcher Kategorie ein Unternehmen gehört, bestimmt sich zunächst nach dem Sektor, in dem das Unternehmen tätig ist. Einige Einrichtungen sind gesondert benannt – Telekommunikationsunternehmen, Vertrauensdiensteanbieter, Top Level Domain Name Registries und DNS-Diensteanbieter. Im Übrigen kommt es darauf an, ob die jeweilige Einrichtung (auch) in einem der in Anlage 1 und Anlage 2 zum BSIG gelisteten Sektoren tätig ist.

10 Empfehlung der Kommission vom 6.5.2003 betreffend die Definition der Kleinstunternehmen sowie der kleineren und mittleren Unternehmen, 2003/361/EG, ABl. L 124, S. 36–41, Art. 2 Abs. 2.
11 *Voigt*, MMR-Aktuell 2021, 437048.
12 Art. 21 NIS-2-Richtlinie.
13 Vgl. etwa *Raffel/Schreiber*, RInPrax 2024, 42, 45.
14 Art. 20 NIS-2-Richtlinie; umfassend dazu auch mit Blick auf die Entwicklung der Umsetzung im deutschen Recht *Schreiber/Brinke*, BB 2024, 2696 ff. Vgl. zur BSI-Handreichung zur Schulungspflicht auch *Teichmann*, BB 2026, 74 ff.
15 BGBl. 2025 I Nr. 301.

In Anlage 1 zum BSIG werden die folgenden Sektoren aufgeführt:
- Energie,
- Transport und Verkehr,
- Finanzwesen,
- Gesundheit,
- Wasser,
- Digitale Infrastruktur,
- Weltraum.

Unternehmen dieser Sektoren gelten, in der Regel abhängig vom Erreichen der jeweiligen Schwellenwerte, als besonders wichtige Einrichtungen.

Anlage 2 beschreibt die sonstigen vom BSIG erfassten Sektoren:
- Post- und Kurierdienste,
- Abfallbewirtschaftung,
- Produktion, Herstellung und Handel mit chemischen Stoffen,
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln,
- Verarbeitendes Gewerbe/Herstellung von Waren,
- Anbieter digitaler Dienste,
- Forschung.

Für Unternehmen dieser Sektoren kommt eine Einordnung als wichtige Einrichtungen in Betracht (§ 28 Abs. 2 Nr. 3 BSIG).

Die jeweiligen Sektoren sind in den Anlagen gesondert definiert. In vielen Fällen wird auf andere EU-Rechtsakte oder auch bestimmte Abteilungen der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) Bezug genommen. Diese Verweisungsketten sind aufzulösen und führen nicht selten, gerade bei Inbezugnahme der NACE Rev. 2, zu einem deutlich erweiterten Adressatenkreis als bei überschlägiger Betrachtung erwartet.

Beispielhaft herausgegriffen seien die Fälle des Managed (Security) Service Providers und der Konzern-IT:

- Erfasst sind Anbieter verwalteter IKT-(Sicherheits)Dienste, sog. Managed (Security) Service Provider (Anlage 1, 6.1.10 und 6.1.11 BSIG). Dies sind nach § 2 Nr. 26 BSIG „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 der Kunden oder aus der Ferne". Ein Managed Security Service Provider bietet diese Tätigkeiten nach § 2 Nr. 25 BSIG „im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit" an. Die Definition ist denkbar weit und umfasst regelmäßig Fälle von Support und Fernwartung, wenn diese mit Zugriffsrechten einhergehen: „Die Rolle des MSP setzt einen gewissen Grad an tatsächlichem Zugriff auf IKT-Produkte, -Netzwerke oder -Infrastrukturen voraus und ist insofern etwa von reinen Beratungstätigkeiten abzugrenzen."[16] Es wird diskutiert, ob bereits die Bereitstellung von Sicherheitsupdates dafür ausreicht.[17] Bei genauer Begriffsbetrachtung kann dies indes – auch in Abgrenzung zur Regulierung des Cyber Resilience Act – nur dann ausreichen, wenn über diese Bereitstellung ein Systemzugriff erfolgt, also nicht nur Updates „per default" ausgespielt werden, sondern auch die gelisteten IKT-Produkte etc. direkt administriert werden, mit einem tatsächlichen Zugriff. Denn nur dann greift nach Sinn und Zweck die Definition, da über den M(S)SP Akteure unter die Regulierung fallen sollen, die durch ihren Zugriff auf Kundensysteme deren Sicherheit maßgeblich mit beeinflussen. Software und andere digitale Produkte einschließlich der für diese bereitgestellten Sicherheitsupdates sind als solche nämlich bereits hinreichend vom Cyber Resilience Act reguliert.
- Derartige Konfigurations- und Administrationsleistungen werden in Unternehmensgruppen häufig von Shared Service Gesellschaften erbracht, die zentral IT-Dienstleistungen anbieten. Auch diese sind regelmäßig als MSP oder MSSP dann allein aufgrund der Leistungserbringung gegenüber verbundenen Unternehmen vom BSIG adressiert: Auch andere Konzerngesellschaften sind „andere" juristische Personen, da in diesem Zusammenhang die unterschiedlichen juristischen Personen und nicht die (gesellschaftsrechtliche) Verbindung zwischen ihnen von Bedeutung sind: Eine Mindestanzahl von Kunden ist keine Voraussetzung für die Einstufung als M(S)SP; die Entwurfsbegründung zum BSIG nennt gerade Unternehmen, die ausschließlich den zentralen IT-Betrieb einer Unternehmensgruppe übernehmen, als typisches Beispiel für einen MSP.[18] Dies steht im Einklang mit den Bestimmungen der NIS-2-Richtlinie, die nur in Fällen eine Ausnahme vorsieht, in denen ein Unternehmen interne Rechenzentren ausschließlich für eigene Zwecke betreibt (Erwägungsgrund 35 NIS-2-Richtlinie).

2. Berechnung der Schwellenwerte

Bestimmte Unternehmen fallen unabhängig von ihrer Größe in den Anwendungsbereich des BSIG, z. B. Telekommunikationsunternehmen, (qualifizierte) Vertrauensdiensteanbieter und Top Level Domain Name Registries oder DNS-Diensteanbieter. In den meisten Fällen müssen Unternehmen zusätzlich zur Geschäftstätigkeit in einem gelisteten Sektor bestimmte Schwellenwerte überschreiten.

Die Einordnung als wichtige Einrichtung setzt dann eine Mitarbeiteranzahl von mindestens 50 Mitarbeitern oder einen Jahresumsatz und eine Jahresbilanzsumme von mehr als 10 Mio. Euro voraus (§ 28 Abs. 2 Nr. 3 BSIG). Als besonders wichtige Einrichtung gilt dann ein Unternehmen, wenn es mindestens 250 Mitarbeiter beschäftigt oder einen Jahresumsatz über 50 Mio. Euro und eine Jahresbilanzsumme über 43 Mio. Euro aufweist (§ 28 Abs. 1 Nr. 4 BSIG).

Allerdings können nur in Anlage 1 gelistete Unternehmen bei Erreichen der höheren Schwellenwerte besonders wichtige Einrichtungen sein (§ 28 Abs. 1 Nr. 4 BSIG); erreichen sie die niedrigeren Schwellen, sind sie (nur) wichtige Einrichtungen (§ 28 Abs. 2 Nr. 3 BSIG). In Anlage 2 gelistete Unternehmen sind stets nur wichtige Einrichtungen, auch wenn sie 250 Mitarbeitende oder mehr beschäftigen oder einen Jahresumsatz von über 50 Mio. Euro und eine Jahresbilanzsumme über 43 Mio. Euro aufweisen (§ 28 Abs. 2 Nr. 3 BSIG).

Eine nur saisonale Überschreitung der Zahlen führt über die Inbezugnahme der Kommissionsempfehlung 2003/361/EG in § 28 Abs. 4 S. 1 BSIG noch nicht zu einer Adressatenstellung: Nach Art. 4 der Kommissionsempfehlung ist grundsätzlich auf den Jahreswert des letzten abgeschlossenen Geschäftsjahres abzustellen. Kommt es dabei erstmalig zu einer Über- oder Unterschreitung der Schwellenwerte, ändert das den Status allerdings erst, wenn diese Über- oder Unterschreitung in zwei aufeinander folgenden Geschäftsjahren vorliegt (Art. 4 Abs. 2 der Kommissionsempfehlung). „Damit führen gegebenenfalls einzelne wirtschaftlich besonders erfolgreiche oder nichterfolgreiche Geschäftsjahre nicht für sich allein zu einer Erfassung als besonders wichtige oder wichtige Einrichtung."[19]

Bei der Berechnung der Schwellenwerte sind gem. § 28 Abs. 4 BSIG allerdings in den meisten Fällen die Zahlen der gesamten Unternehmensgruppe zu addieren, auch wenn die Adressatenstellung mit Registrierungspflichten etc. jeweils nur einen einzelnen Rechtsträger betrifft: Die Daten verbundener Unternehmen und von Partnerunternehmen, jeweils nach Maßgabe der Empfehlung der Kommission

16 BT-Drs. 21/1501, 132.
17 *Hessel/Schneider*, MMR 2025, 243, 244.
18 BT-Drs. 21/1501, 132; dahingehend auch *Dittrich/Kipker*, MMR-Aktuell 2025, 01362; *Hessel/Schneider*, MMR 2025, 243, 244; *Hessel/Callewaert/Schneider*, RDi 2024, 208, 209; *Leßner*, MMR 2024, 226, 227.
19 BT-Drs. 21/1501, 145.

2003/361/EG bestimmt, die im Wesentlichen §§ 15 ff. AktG ähnelt, sind zusammenzurechnen. Dies gilt nach § 28 Abs. 4 S. 2 BSIG nur dann nicht, „wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist". Von einer solchen Unabhängigkeit ist ausweislich der Entwurfsbegründung auszugehen, „wenn grundsätzliche Entscheidungen zur Beschaffung, zum Betrieb und zur Konfiguration der informationstechnischen Systeme, Komponenten und Prozesse durch die Einrichtung eigenverantwortlich getroffen werden können".[20] Das ist dann nicht der Fall, wenn die Konzernmutter ein einheitliches IT-System für die gesamte Gruppe vorsieht.

Ursprünglich war noch vorgesehen, dass die Berechnung der Schwellenwerte für die Adressatenstellung allein auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit abgestellt werden sollte.[21] Die Vereinbarkeit dieser Regelung mit der NIS-2-Richtlinie war indes umstritten.

3. Ausnahme für vernachlässigbare Geschäftstätigkeiten

Beachtenswert ist eine Sonderregelung hinsichtlich des Anwendungsbereichs des BSIG: Nach § 28 Abs. 3 BSIG sollen bei der Zuordnung einer Einrichtung zu einem der regulierten Sektoren bzw. Tätigkeiten, solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung *vernachlässigbar* sind. Ausweislich der Gesetzesbegründung soll so im Einzelfall vermieden werden, dass nur eine geringfügige Nebentätigkeit zu einer unverhältnismäßigen Identifizierung als wichtige oder besonders wichtige Einrichtung führt. Anhaltspunkte für „vernachlässigbare" Geschäftstätigkeiten können etwa die Anzahl der in dem betroffenen Bereich tätigen Mitarbeiter sein, der durch die Geschäftstätigkeit erwirtschaftete Umsatz oder die Bilanzsumme für diesen Bereich. Indiz für eine Geschäftstätigkeit, die nicht „vernachlässigbar" ist, ist ihre Nennung in einem Gesellschaftervertrag, einer Satzung oder einem vergleichbaren Gründungsdokument. Entscheidend soll das Gesamtbild der betreffenden Geschäftstätigkeit im Lichte der Gesamtgeschäftstätigkeit der Einrichtung unter Berücksichtigung aller relevanter Anhaltspunkte sein.[22]

Zum Teil wird in Frage gestellt, ob diese Regelung EU-rechtskonform ist. Die NIS-2-Richtlinie enthält keine Ausnahme für „vernachlässigbare Geschäftstätigkeiten". Allerdings ist in mehreren Erwägungsgründen angesprochen, dass unverhältnismäßige Belastungen vermieden werden sollen (z. B. Erwägungsgründe 16, 21, 81, 82 NIS-2-Richtlinie). Hierüber könnte argumentiert werden, dass die Ausnahme für vernachlässigbare Geschäftstätigkeiten mit den Vorgaben der NIS-2-Richtlinie vereinbar ist. Eindeutig ist dies jedenfalls nicht. Der deutsche Gesetzgeber hat trotz kritischer Stimmen im Laufe des Gesetzgebungsverfahrens bis zum Schluss an der Ausnahmeregelung festgehalten. Wäre die Regelung EU-rechtswidrig, dürfte sie aufgrund des Anwendungsvorrangs des EU-Rechts nicht angewendet werden, auch nicht vom BSI. Bislang gibt es aber keine Anhaltspunkte, dass das BSI von einer Unanwendbarkeit ausgehen würde. Dies spricht dafür, dass auch das BSI sich in der behördlichen Praxis zunächst hieran orientieren wird und sie daher auch in der Praxis angewendet werden kann.

Auch die Anwendung der Ausnahmeregelung bringt Rechtsunsicherheiten mit sich: Trotz der Anhaltspunkte in der Gesetzesbegründung erscheint es schwierig, trennscharf eine „vernachlässigbare" Tätigkeit zu bestimmen, insbesondere, da Rechtsprechung und konkrete behördliche Leitlinien zu dieser Ausnahmeregelung bisher fehlen. Erforderlich ist eine wertende Gesamtbetrachtung, die eindeutig eine „Vernachlässigbarkeit" der Tätigkeit belegen, sie also als für die gesamte Einrichtung unwesentlich und nebensächlich ausweisen muss. Indizien dafür können die fehlende Nennung im Unternehmenszweck sein sowie die mit Blick auf Umsatz und Ressourcenaufwand nur unwesentliche Bedeutung sein. Zudem sollte das von den Entwurfsverfassern angeführte Beispiel wertend verglichen werden: Ein Unternehmen, das auch eine PV-Anlage betreibt, soll nicht nur deswegen in den Adressatenkreis des BSIG (Stromerzeugung) gelangen. Wenn etwa ein Logistikunternehmen auch eine PV-Anlage auf einer Halle betreibt, liegt es auf der Hand, dass dies nicht die zentrale Geschäftstätigkeit ist. Eine Entscheidung gegen die Betroffenheit auf Grundlage der Ausnahmeregelung des § 28 Abs. 3 BSIG bedarf angesichts dessen einer umfassenden Gesamtabwägung und muss sorgfältig begründet und dokumentiert werden.

4. Einrichtungen der Bundesverwaltung

Ein wesentlicher Kritikpunkt im Rahmen der NIS-2-Umsetzung war immer wieder, dass die Einrichtungen der Bundesverwaltung ungerechtfertigt gegenüber der Wirtschaft privilegiert und zu weniger weitreichenden Cybersicherheitsmaßnahmen verpflichtet würden. Die Systematik des § 28 BSIG gilt in der Tat nicht für Einrichtungen der Bundesverwaltung. Solche sind weder besonders wichtige Einrichtungen noch wichtige Einrichtungen.

Ausgenommen sind sie indes ebenfalls nicht, sondern über § 29 BSIG vom neuen Informationssicherheitsrechts adressiert, konkret

- Bundesbehörden,
- öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung und
- weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts auf Bundesebene sowie ihre Vereinigungen, soweit durch das BSI im Einvernehmen mit dem jeweils zuständigen Ressort angeordnet (§ 29 Abs. 1 BSIG[23]).

Erleichterungen gibt es für diese Einrichtungen in der Regulierung aber nicht nur über die Begrenzung auf die Anordnung in der dritten Fallgruppe, sondern auch über § 29 Abs. 2, 3 BSIG, der einige Regelungen des BSIG für unanwendbar auf diese Einrichtungen erklärt. Insofern findet die Kritik wegen der Privilegierung dieser Einrichtungen nach wie vor eine Grundlage.

III. Registrierungspflicht

Ist ein Unternehmen als wichtige oder besonders wichtige Einrichtung von § 28 BSIG erfasst, greift die Registrierungspflicht des § 33 BSIG spätestens drei Monate nachdem es erstmals oder erneut von den Pflichten des BSIG betroffen ist.

Für die Registrierung sieht das BSI ein zweistufiges Verfahren vor: Zunächst muss „Mein Unternehmenskonto (MUK)" eingerichtet werden. Mit diesen Login-Daten kann sich das Unternehmen dann im sog. BSI-Portal einloggen, unter https://portal.bsi.bund.de/, und die Registrierung vervollständigen sowie im Nachgang etwa auch erforderliche Meldungen abgeben.

20 BT-Drs. 21/1501, 145.
21 Gesetzentwurf vom 2.10.2024.
22 BT-Drs. 21/1501, 144.
23 BT-Drs. 21/1501, 147.

Bei der Registrierung sind nach § 33 Abs. 1 Nr. 1-5 BSIG anzugeben:
- Name der Einrichtung einschließlich Rechtsform und, falls einschlägig, Handelsregisternummer,
- Anschrift und Kontaktdaten einschließlich E-Mail-Adresse, öffentliche IP-Adressbereiche und Telefonnummern,
- relevanter Sektor, Teilsektor oder Branche nach Anlage 1 oder 2 zum BSIG,
- EU-Mitgliedstaaten, in denen die betroffene Einrichtung BSIG-relevante Dienste erbringt,
- die für die Tätigkeiten, aufgrund derer die Registrierung erfolgt, zuständigen Aufsichtsbehörden des Bundes und der Länder.

Anbieter bestimmter Einrichtungsarten sind zu weitergehenden Angaben verpflichtet, u. a. Betreiber kritischer Anlagen (§ 33 Abs. 2 BSIG) und Anbieter digitaler Dienste (§§ 34, 60 Abs. 1 S. 1 BSIG).

Änderungen dieser Angaben müssen grundsätzlich unverzüglich, spätestens aber innerhalb von zwei Wochen mitgeteilt werden (§ 33 Abs. 5 BSIG).

Wer die Registrierungspflicht schuldhaft nicht einhält, kann nach § 65 Abs. 2 Nr. 6, Abs. 5 Nr. 5 BSIG mit einem Bußgeld in Höhe von bis zu 500 000 Euro belegt werden. Bestehen insofern Zweifel, ist das BSI zur Anforderung von Informationen zur Sachverhaltsaufklärung befugt.[24]

Die Registrierungspflicht gilt auch für die von § 28 BSIG erfassten Einrichtungen, die bereits sektorspezifischen Cybersicherheitspflichten unterliegen, z. B. Finanzunternehmen oder Telekommunikationsdiensteanbietern. Für diese Sektorunternehmen sehen die Absätze 5 und 6 des § 28 BSIG zwar diverse Ausnahmen vom BSIG vor, § 33 BSIG ist aber gerade nicht ausgenommen. So wird abgesichert, dass das BSI einen umfassenden Überblick über die Gesamtzahl der Einrichtungen erhält, die nach Ansicht des EU-Richtliniengebers für die Cyberresilienz der EU eine besondere Bedeutung haben.

IV. Risikomanagement

Wichtige und besonders wichtige Einrichtungen sind zu umfassenden Risikomanagementmaßnahmen verpflichtet (§ 30 BSIG). Die Norm bildet das Herzstück des neuen Informationssicherheitsrechts: Implementiert werden müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit informationstechnischer Systeme, Komponenten und Prozesse zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Gefordert wird damit ein Informations-Sicherheits-Management, das die materielle Informationssicherheit der Einrichtung angemessen ausgestaltet.

§ 30 Abs. 2 BSIG enthält eine Reihe an typischerweise („mindestens“) erforderlichen Maßnahmen:
- Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
- Bewältigung von Sicherheitsvorfällen,
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
- grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
- Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
- Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Die gewählten Maßnahmen „sollen“ nach dem Wortlaut des § 30 Abs. 2 BSIG den Stand der Technik einhalten, einschlägige Normen berücksichtigen und insgesamt auf einem gefahrübergreifenden Ansatz beruhen. Art. 21 Abs. 1 UAbs. 2 NIS-2-Richtlinie verlangt insofern eine Berücksichtigung des Stands der Technik. Dies ist auch aus Art. 32 DSGVO bekannt[25] und wird – dem allgemeinen Sprachverständnis folgend – dahingehend ausgelegt, dass es jeweils im Einzelfall zu bewerten ist, ob Maßnahmen, um angemessen zu sein, den Stand der Technik einhalten müssen, hinter diesem zurückbleiben können – wegen geringer Risikoexposition – oder bei besonders hohem Risiko womöglich sogar darüber hinausgehen müssen.[26] In der Abwägung, welche Risikomanagementmaßnahmen verhältnismäßig und angemessen sind, müssen insbesondere das Ausmaß der Risikoexposition, die Größe des Unternehmens, die Umsetzungskosten, die Wahrscheinlichkeit des Eintritts von Sicherheitsvorfällen und ihre Schwere berücksichtigt werden.

Regelmäßig wird es sich anbieten, die Maßnahmen anhand der einschlägigen und anerkannten technischen Regelwerke abzubilden, dem BSI-Grundschutzkompendium und der ISO27001. Dies können indes immer nur Anhaltspunkte sein, die den Stand der Technik illustrieren. Im Einzelfall kann die genaue Risikoanalyse und Bewertung dazu führen, dass andere Maßnahmen ergriffen werden müssen, die auch hinter den Regelwerken zurückbleiben oder über diese hinausgehen können. Die Darlegungs- und Beweislast für ein angemessenes Risikomanagement liegt nach § 30 Abs. 1 S. 3 BSIG bei der adressierten Einrichtung.

Einrichtungen, die zwar von § 28 BSIG erfasst, zugleich aber auch sektorspezifisch sicherheitsreguliert sind, müssen die Vorgaben des § 30 BSIG regelmäßig nicht einhalten: Nach § 28 Abs. 5, 6 BSIG gelten die Pflichten des § 30 BSIG nicht für Unternehmen aus dem Telekommunikations- und Energiesektor, Finanzunternehmen und die Gesellschaft für Telematik. Dies bedeutet indes nicht, dass diese Einrichtung keine angemessenen Risikomanagementmaßnahmen implementieren müssen, vermieden wird lediglich eine Doppelregulierung. Denn vergleichbare Pflichten finden sich für diese Unternehmen in den sektorspezifischen Vorgaben, z. B. § 165 TKG in der Fassung vom 2.12.2025 nach Art. 25 NIS2UmsuCG.

Auch für die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz gilt § 30 BSIG nach § 29 Abs. 3 BSIG nicht.

V. Pflichten der Leitungsorgane

Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind nach § 38 Abs. 1 BSIG verpflichtet, die von diesen

24 § 33 Abs. 4 BSIG, s. dazu *Nink*, Das neue IT-Sicherheitsrecht, 2026, § 4, Rn. 28.
25 S. ausführlich zum Verhältnis von NIS-2-Richtlinie und DSGVO *Schreiber*, CR 2025, 647 ff.
26 Vgl. mit Verweis auf Art. 32 DSGVO *Nink*, Das neue IT-Sicherheitsrecht, 2026, § 3, Rn. 8.

Einrichtungen nach § 30 BSIG zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen. § 38 BSIG findet seine Grundlage in Art. 20 NIS-2-Richtlinie und war im Entstehungsprozess des neuen Gesetzes einer umfassenden Evolution ausgesetzt.[27] Art. 20 NIS-2-Richtlinie spricht anders als der deutsche Umsetzungsakt von der Pflicht, die Risikomanagementmaßnahmen zu „billigen", also nicht selbst herauszuarbeiten und zu implementieren, was „umsetzen" suggeriert, sondern zu begleiten, zu plausibilisieren und für gut zu heißen. Ebenso will indes auch die Entwurfsbegründung § 38 Abs. 1 BSIG verstanden wissen: „Nach dieser Verpflichtung haben die Geschäftsleitungen die konkret zu ergreifenden Maßnahmen zunächst als für geeignet zu billigen und deren Umsetzung kontinuierlich zu überwachen."[28] Dies ermöglicht die Delegation auf Hilfspersonen, allerdings bleibt die Führungsebene auch dann letztverantwortlich.[29]

Verletzt die Leitungsebene ihre Pflichten aus § 38 Abs. 1 BSIG, haftet sie dem Unternehmen dafür persönlich. Gem. § 38 Abs. 2 BSIG folgt dies grundsätzlich aus den allgemeinen Haftungsregeln, also je nach Gesellschaftsform etwa beispielsweise aus § 43 GmbHG. Nur wenn eine solche Haftungsnorm fehlt, bildet § 38 Abs. 2 BSIG die Haftungsgrundlage.[30] Die persönlichen Haftungsrisiken können über eine D&O-Versicherung abgedeckt werden; auch dies war im Gesetzgebungsprozess zunächst umstritten, ist aber bestätigt worden.

Damit die Leitungsebene ihren Pflichten genügen kann, sieht § 38 Abs. 3 BSIG eine regelmäßige Schulungspflicht vor. Diese erfordert in der Regel alle drei Jahre[31] eine Veranstaltung, durch die die Leitungsebene befähigt wird, Risiken und Risikomanagementmaßnahmen konkret zu bewerten. Durchführen kann diese Veranstaltung jede Person, die ausreichende Fähigkeiten vermitteln kann; dies kann auch der eigene CISO sein oder aber eine externe Schulungsakademie. Nach den Vorgaben des BSI erfordert die NIS-2-Geschäftsleitungsschulung einen rechtlichen Überblick, die Befähigung zur Risikoanalyse und Bewertung von Risikomanagementmaßnahmen.[32]

VI. Meldepflichten

Ein erheblicher Sicherheitsvorfall löst für wichtige und besonders wichtige Einrichtungen Meldepflichten gegenüber dem BSI nach § 32 BSIG aus. Derartige Meldepflichten sind aus der DSGVO bereits für eine Vielzahl von Adressaten bekannt. Anders als unter der DSGVO sieht das BSIG allerdings eine mehrstufige Meldepflicht vor:

- Frühe Erstmeldung: Spätestens 24 Stunden nach Kenntniserlangung von dem jeweiligen Vorfall erfolgt eine erste Meldung (sog. Frühwarnung).
- Detaillierte Meldung: Auch unverzüglich, spätestens jedoch 72 Stunden nach Kenntniserlangung, muss eine offizielle Meldung über den Vorfall einschließlich einer ersten Bewertung des Schweregrads und der Auswirkungen an das BSI erfolgen.
- Abschlussmeldung: Spätestens einen Monat nach Übermittlung dieser Meldung ist ein Abschlussbericht abzugeben. Dieser muss den Sicherheitsvorfall ausführlich beschreiben, die Art der Bedrohung und die wahrscheinliche Ursache sowie ergriffene Abhilfemaßnahmen. Für den Fall grenzüberschreitender Auswirkungen des Vorfalls müssen auch diese im Abschlussbericht enthalten sein. Sollte der Vorfall zu diesem Zeitpunkt noch andauern, wird stattdessen ein Fortschrittsbericht abgegeben.

Zu melden sind nur erhebliche Sicherheitsvorfälle, also solche, die den Betrieb eines Dienstes schwerwiegend beeinträchtigen, finanzielle Schäden für die erbringende Einrichtung oder erhebliche materielle oder immaterielle Schäden für andere Personen oder Unternehmen verursachen können (§ 2 Nr. 11 BSIG).

Für DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste (Managed Service Provider – MSP), Anbieter verwalteter Sicherheitsdienste (Managed Security Service Provider – MSSP), Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke sowie Vertrauensdiensteanbieter konkretisiert die Durchführungsverordnung (EU) 2024/2690 der Kommission, kurz NIS2-DVO, wann ein Sicherheitsvorfall erheblich ist und welche Risikomanagementmaßnahmen ergriffen werden müssen. Die NIS2-DVO gilt zwar nicht für alle Adressaten des BSIG, kann aber mit Ausstrahlungswirkung auch für nicht direkt adressierte Einrichtungen als Auslegungshilfe herangezogen werden. So sind etwa nach Art. 3 Abs. 1 lit. a NIS2-DVO Sicherheitsvorfälle erheblich, wenn der Vorfall zu einem direkten finanziellen Verlust der betroffenen Einrichtung in Höhe von mehr als 500 000 Euro oder 5 % ihres jährlichen Gesamtumsatzes im vorangegangenen Geschäftsjahr – je nachdem, welcher Wert niedriger ist – führt oder führen kann. Konkret für Anbieter von Cloud-Computing-Diensten reicht bereits die flächendeckende Nichtverfügbarkeit über 30 Minuten (Art. 7 lit. a NIS2-DVO).

Derzeit sind die Meldepflichten nach BSIG parallel zu jenen etwa nach Art. 33 DSGVO durchzuführen. Mit dem Digital Omnibus on digital aquis plant die Kommission hier eine Erleichterung und die Einrichtung eines einzigen zentralen Online-Meldeportals, über das die Informationen dann an alle Behörden geleitet werden, die zu informieren sind.[33]

Das BSI kann im Einzelfall anordnen, dass auch die Empfänger der Dienste besonders wichtiger und wichtiger Einrichtungen unverzüglich durch diese zu unterrichten sind, was auch durch eine Veröffentlichung auf der Internetseite der Einrichtung erfolgen kann (§ 35 Abs. 1 BSIG). Betroffenen Empfängern der kompromittierten Dienste sind, unter Umständen auch ohne Aufforderung durch das BSI, Abhilfemaßnahmen an die Hand zu geben, die diese als Reaktion auf eine Cyberbedrohung ergreifen können (§ 35 Abs. 2 BSIG).

VII. Konsequenzen bei Verstößen

Bei Verstößen gegen die Vorschriften des BSIG drohen Bußgelder von bis zu 10 Mio. Euro oder 2 % des erzielten Jahresumsatzes, je nachdem, welcher Betrag höher ist (§ 65 BSIG). Sanktionen für wichtige Einrichtungen können einen Betrag von bis zu 7 Mio. Euro oder 1,4 % des erzielten Jahresumsatzes erreichen (§ 65 Abs. 5 Nr. 1 lit. b, Abs. 7 BSIG).

Das BSI wird zudem mit erweiterten Aufsichts- und Durchsetzungsbefugnissen ausgestattet (§§ 61, 62 BSIG). Gegenüber besonders wichtigen Einrichtungen können u. a. die folgenden Maßnahmen angeordnet bzw. ergriffen werden:

27 Umfassend dazu *Schreiber/Brinke*, BB 2024, 2696 ff.
28 BT-Drs. 21/1501, 154.
29 BT-Drs. 21/1501, 154.
30 Ausführlich *Schreiber/Brinke*, BB 2024, 2696, 2700 ff.
31 BT-Drs. 21/1501, 154.
32 BSI, Handreichung NIS-2-Geschäftsleitungsschulung vom 30.9.2025, unter https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Geschaeftsleitungsschulung/NIS-2-Geschaeftsleitungsschulung_node.html (Abruf: 23.1.2026). Vgl. hierzu auch *Teichmann*, BB 2026, 74 ff.
33 COM(2025) 837 final, S. 65 mit dem Vorschlag für einen neuen Art. 23a NIS-2-Entwurf: „Single-entry point for incident reporting".

– Verpflichtende Audits und Prüfungen, einschließlich Vor-Ort-Kontrollen (§ 61 Abs. 1, Abs. 5 BSIG),
– Anforderung von Informationen und Nachweisen zur Bewertung von Risikomanagementmaßnahmen, z. B. mit Blick auf die Umsetzung von Cybersicherheitskonzepten (§ 61 Abs. 3, Abs. 4 BSIG),
– Verbindliche Anweisungen, insbesondere zur Ergreifung von Maßnahmen bei einem Sicherheitsvorfall, ggf. unter Fristsetzung (§ 61 Abs. 7, Abs. 8 BSIG),
– Genehmigungen aussetzen (§ 61 Abs. 9 S. 2 Nr. 1 BSIG),
– Vorübergehende Untersagung der Leitung gegenüber Geschäftsführungen (§ 61 Abs. 9 S. 2 Nr. 2 BSIG).

VIII. Ausblick

Die Verpflichtungen des BSIG gelten für eine Vielzahl von Unternehmen, in denen auch die Leitungsorgane nunmehr bestätigt persönlich haftend für eine ausreichende Informationssicherheit Rechnung zu tragen haben. Die Betroffenheitsanalyse ist daher Compliance-Grundanforderung für das Management, die Umsetzung angemessener Risikomanagementmaßnahmen für beinahe alle Unternehmen Pflicht – entweder bußgeldbewehrt über eine Adressatenstellung unter dem BSIG oder aber als vertragliche Pflicht in der Lieferkette eines BSIG-Adressaten oder jedenfalls als allgemeine Compliance-Pflicht angesichts wachsender Bedrohungen. Die Informationssicherheit sollte angesichts dessen bei jedem Unternehmen auf dem Prüfstand stehen.

Dr. Kristina Schreiber, RAin/FAinVerwR, ist Partnerin und CIPP/E bei Loschelder Rechtsanwälte in Köln sowie Lehrbeauftragte an der Universität Köln und der Fernuniversität Hagen. Sie ist spezialisiert auf die Begleitung von Digitalisierungsprojekten mit regulatorischem Beratungsschwerpunkt auf IT-Sicherheit, KI, Datenschutz und Datennutzung.

Marvin Schäfer

Kapitalaufbringungsgrundsatz im Lichte von Online-Zahlungsdienstleistungen, E-Geld und Kryptowährungen

Der Kapitalaufbringungsgrundsatz und die sich daraus ergebenden Einlageverpflichtungen sind sowohl bei der Gesellschaft mit beschränkter Haftung (GmbH) als auch bei der Aktiengesellschaft (AG) von zentraler Bedeutung. Rechtlich weithin unproblematisch sind dabei diejenigen Fälle, in denen geläufige Zahlungsmittel zur Aufbringung des Kapitals der Gesellschaft verwendet werden. Demgegenüber wirft die dynamische Entwicklung im Bereich von Online-Zahlungsdienstleistungen, sog. E-Geld und Kryptowährungen, spannende und zum Teil komplexe Rechtsfragen auf. Ob dem Kapitalaufbringungsgrundsatz auch bei der Verwendung von Online-Zahlungsdienstleistungen, E-Geld und Kryptowährungen hinreichend Rechnung getragen werden kann und welche Besonderheiten hierbei zu beachten sind, erläutert dieser Beitrag.

I. Kapitalaufbringungsgrundsatz im Allgemeinen

Der Kapitalaufbringungsgrundsatz ist eines der wesentlichen Elemente, das in unterschiedlichen Stadien einer Kapitalgesellschaft von besonderer Relevanz ist.[1] Bereits bei der Gründung einer Kapitalgesellschaft stellen sich bedeutsame Fragen zur Aufbringung des maßgeblichen Kapitals, die sich dann auch auf entsprechende Erhöhungen des Grundkapitals erstrecken.

Die wohl relevantesten Rechtsformen unter den Kapitalgesellschaften bilden dabei die GmbH und die AG, auf deren im Gründungsstadium bestehenden rechtlichen Besonderheiten im Zusammenhang mit der Kapitalaufbringung sich dieser Beitrag konzentriert.

1. GmbH

Seine normative Verankerung hat der Grundsatz der Kapitalaufbringung für die GmbH in § 7 Abs. 2 GmbHG.[2] Danach darf die Anmeldung der Gesellschaft erst erfolgen, wenn auf jeden Geschäftsanteil ein Viertel des Nennbetrages eingezahlt ist. Insgesamt muss auf das Stammkapital mindestens so viel eingezahlt sein, dass der Gesamtbetrag der eingezahlten Geldeinlagen zuzüglich des Gesamtnennbetrags der Geschäftsanteile, für die Sacheinlagen zu leisten sind, die Hälfte des Mindeststammkapitals gemäß § 5 Abs. 1 GmbHG erreicht. Das Mindest-Stammkapital beläuft sich nach § 5 Abs. 1 GmbHG auf 25 000 Euro.

Hinter der Vorschrift des § 7 Abs. 2 GmbHG steht der Gedanke, dass die Gesellschaft bei ihrer Gründung mit einem gewissen Mindestbetrag an finanziellen Mitteln zur freien Verfügung ausgestattet ist.[3]

Das Gesetz unterscheidet insoweit zwischen der sich daraus ergebenden Einlageverpflichtung in Gestalt der sog. Bareinlage und der sog. Sacheinlage.[4]

a) Bareinlageverpflichtung

Die Verpflichtung zur Kapitalaufbringung wird regelmäßig durch eine Bareinlage (auch sog. Geldeinlage) erfüllt. Insoweit ist – entgegen dem

1 *Altmeppen*, in: Altmeppen, GmbHG, 11. Aufl. 2023, § 7, Rn. 23 ff.; *Koch*, in: Koch, AktG, 19. Aufl. 2025, § 1, Rn. 11.
2 *Altmeppen*, in: Altmeppen, GmbHG, 11. Aufl. 2023, § 7, Rn. 23.
3 *Casper*, in: Habersack/Casper/Löbbe, GmbHG Großkommentar, 4. Aufl. 2025, Bd. 1, § 7, Rn. 2.
4 *Müther*, in: BeckOGK, Stand: 1.7.2025, GmbHG § 7, Rn. 44 ff., 58 ff.