DataAgenda-Arbeitspapier 85, 8/2026

DataAgenda - das Lösungsportal
zum Datenschutzrecht

Präsentiert von DATAKONTEXT

www.DataAgenda.de

Die neue Rechtslage der unternehmerischen IT-Sicherheit zwischen NIS-2-Richtlinie, neuem BSI-Gesetz und flankierenden Regelungen

I. Einleitung

Die fortschreitende Digitalisierung von Wirtschaft und Verwaltung hat die Angriffsflächen für Cyberattacken erheblich vergrößert. Zugleich sind Cyberangriffe im Kontext geopolitischer und zwischenstaatlicher Konflikte zu einem strukturellen Risiko geworden, das den unternehmerischen Alltag prägt. Der Gesetzgeber reagiert auf diese Entwicklung mit einer deutlichen Verschärfung und Ausweitung der rechtlichen Anforderungen an die IT-Sicherheit.

Mit dem Inkrafttreten des NIS-2-Umsetzungsgesetzes am 6. Dezember 2025 hat sich das deutsche Recht der IT-Sicherheit grundlegend verändert. Der Kreis der unmittelbar verpflichteten Unternehmen ist von rund 1.600 auf etwa 30.000 Einrichtungen angewachsen. IT-Sicherheit ist damit von einer technischen Aufgabe einzelner Fachabteilungen zu einer verbindlichen Compliance-Pflicht der Unternehmensleitung geworden.

Im Zentrum der neuen Regulierung steht ein Perspektivwechsel: IT-Sicherheit wird nicht länger als delegierbare Aufgabe der IT-Abteilung verstanden, sondern als integraler Bestandteil der Unternehmensführung und des Risikomanagements. Die Verantwortung dafür weist das Gesetz ausdrücklich der Geschäftsleitung zu, verbunden mit einer persönlichen Haftung und einer eigenständigen Schulungspflicht. Cybersicherheit ist damit zur Chefsache geworden.

II. Gefährdungsbild und Schutzziele

1. Bedrohungen und Schadensfolgen

Gefahren für die IT-Sicherheit gehen sowohl von Innentätern als auch von externen Akteuren aus — etwa Hackern, Schadsoftware und automatisierten Angriffen — sowie von reinen Systemstörungen. Realisieren sich diese Gefahren, drohen wirtschaftliche Schäden, ein Verlust der Reputation und rechtliche Konsequenzen. Der Verlust der Datensicherheit ist damit nicht nur ein technisches, sondern ein existenzielles unternehmerisches Risiko.

Der Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) für das Jahr 2025 bestätigt ein angespanntes Sicherheitsniveau. Mit der fortschreitenden Digitalisierung wachsen schlecht geschützte Angriffsflächen, und im Kontext geopolitischer Konflikte nehmen die Aktivitäten sogenannter Advanced Persistent Threats (APT) zu. Für die Wirtschaft zählen Ransomware, Abhängigkeiten innerhalb der IT-Lieferkette sowie offene oder falsch konfigurierte Onlineserver zu den größten Bedrohungen; die Gesellschaft ist vor allem von Identitätsdiebstahl, Sextortion und Phishing betroffen.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

2. Die Schutzziele der Informationssicherheit

IT-Sicherheit und Datensicherheit lassen sich anhand von vier Schutzzielen beschreiben, die den Maßstab für angemessene Sicherheitsmaßnahmen bilden:

- **Vertraulichkeit:** Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
- **Integrität:** Daten müssen vollständig und unverändert bleiben.
- **Verfügbarkeit:** Dienstleistungen, Funktionen und Informationen müssen dem Benutzer zum geforderten Zeitpunkt zur Verfügung stehen.
- **Belastbarkeit (Resilienz):** Die Informationstechnik muss im Fehlerfall, bei Störungen und bei hoher Beanspruchung widerstandsfähig sein.

III. Die Rechtslage bis 2025

1. Unübersichtlichkeit gesetzlicher Verpflichtungen

Unternehmen waren bereits vor der NIS-2-Umsetzung über eine Vielzahl gesetzlicher Regelungen zum Risikomanagement einschließlich eines angemessenen IT-Sicherheitsniveaus verpflichtet. Von besonderer Bedeutung waren das KonTraG, das bis 2025 eine wichtige Grundlage für Aktiengesellschaften, GmbHs und Unternehmen im Anwendungsbereich des HGB bildete und bei Verstößen eine persönliche Haftung von Vorstand, Aufsichtsrat und Geschäftsführung vorsah, sowie die Datenschutz-Grundverordnung mit ihren Anforderungen an Datensicherheit und datenschutzfreundliche Technikgestaltung (Art. 25 Abs. 1 und Art. 32 DS-GVO). Hinzu kamen bereichsspezifische Vorgaben etwa aus dem TDDDG (§ 18 Abs. 4), dem TKG (§ 165 Abs. 1 Satz 2), der KritisVO als Teil des IT-Sicherheitsgesetzes 2015 sowie für den Finanzsektor die europäische DORA-Verordnung.

Die praktische Wirkung dieser Vorgaben blieb allerdings begrenzt. Die Pflichten waren häufig zu allgemein gefasst, um ein spürbar höheres IT-Sicherheitsniveau zu bewirken.

2. Das IT-Sicherheitsgesetz 2015 und das alte BSIG

Einen wichtigen Schritt markierte das erste IT-Sicherheitsgesetz von 2015. Es betraf allerdings überwiegend nur Betreiber kritischer Infrastrukturen (KRITIS) — also Unternehmen, deren Anlagen in der Regel mehr als 500.000 Personen versorgen. Kritische Infrastrukturen im Sinne des alten BSIG waren Einrichtungen und Anlagen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Siedlungsabfallentsorgung sowie Finanz- und Versicherungswesen. Als „kritisch“ galt eine Anlage, wenn ihr Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe verursachen oder die öffentliche Sicherheit gefährden könnte; welche Einrichtungen konkret erfasst waren, ergab sich aus der KritisVO.

3. Pflichten und Rechtsfolgen nach altem Recht

Betreiber kritischer Infrastrukturen trafen nach dem alten BSIG besondere Pflichten. Dazu gehörten die Einhaltung von Mindeststandards der technischen Sicherheit nach dem Stand der Technik, der Einsatz von Systemen zur Angriffserkennung, die Meldung von Störungen, Schadprogrammen und Hackerangriffen an das BSI, der Nachweis der Einhaltung gesetzlicher Vorgaben mindestens alle zwei Jahre wie etwa durch Audit, Prüfung oder Zertifizierung, die Registrierung beim BSI nebst Benennung einer jederzeit erreichbaren Kontaktstelle, die Vorlage erforderlicher Unterlagen sowie besondere Pflichten beim Einsatz kritischer Komponenten, etwa in Gestalt einer Garantieerklärung des Herstellers.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Die Rechtsfolgen bei Verstößen waren in § 14 BSIG a.F. geregelt. Bei nicht beseitigten Sicherheitsmängeln drohten Geldbußen von bis zu 2.000.000 Euro. Als Kritikpunkte am alten Regime galten insbesondere unklare Speicherfristen beim BSI, unklare Zwecke und Empfänger von Datenübermittlungen sowie eine nicht ausreichende Unabhängigkeit des BSI. Insgesamt war das alte Recht ein Schritt in die richtige Richtung, in seiner Reichweite und Bestimmtheit aber unzureichend.

IV. Die europäische Neuregelung: Die NIS-2-Richtlinie

1. Zielsetzung und Anwendungsbereich

Die NIS-2-Richtlinie ist die EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. Sie ersetzt die erste NIS-Richtlinie und weitet den Kreis der erfassten Sektoren und Einrichtungen erheblich aus. Der amtliche Richtlinientext ist über EUR-Lex abrufbar (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555).

Die Richtlinie unterscheidet zwischen Sektoren mit hoher Kritikalität und sonstigen kritischen Sektoren. Zu den Sektoren mit hoher Kritikalität zählen Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser und Abwasser, digitale Infrastruktur, die Verwaltung von IKT-Diensten im Geschäftskundenbereich, die öffentliche Verwaltung sowie der Weltraum. Zu den sonstigen kritischen Sektoren gehören Post- und Kurierdienste, Abfallbewirtschaftung, die Produktion und der Handel mit chemischen Stoffen, die Produktion, Verarbeitung und der Vertrieb von Lebensmitteln, das verarbeitende Gewerbe, Anbieter digitaler Dienste sowie die Forschung.

2. Wesentliche und wichtige Einrichtungen

Die NIS-2-Richtlinie unterscheidet nach Art. 3 zwischen „wesentlichen“ und „wichtigen“ Einrichtungen. Ob eine Einrichtung erfasst ist, hängt regelmäßig von der Kombination aus Sektorzugehörigkeit und einem Schwellenwert ab: In der Regel greift die Richtlinie ab mindestens 50 Beschäftigten oder einem Jahresumsatz von mehr als 10 Millionen Euro. Nicht erfasst sind unter anderem die Bereiche Verteidigung, nationale und öffentliche Sicherheit, Strafverfolgung und Justiz; auch Parlamente und Zentralbanken sind ausgenommen.

3. Pflichten der Mitgliedstaaten

Art. 7 Abs. 1 NIS-2-RL verpflichtet jeden Mitgliedstaat, eine nationale Cybersicherheitsstrategie zu erlassen. Die Vorschrift lautet:

“Jeder Mitgliedstaat erlässt eine nationale Cybersicherheitsstrategie, die die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus enthält.“

Nach Art. 7 Abs. 2 NIS-2-RL bilden dabei unter anderem die Aufrechterhaltung eines offenen Internets, die Förderung neuer Technologien für das Risikomanagement, die Förderung der allgemeinen und beruflichen Bildung im Bereich Cybersicherheit sowie die Stärkung der Cyberresilienz und Cyberhygiene kleiner und mittlerer Unternehmen inhaltliche Schwerpunkte.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

4. Risikomanagement- und Meldepflichten

Nach Art. 21 NIS-2-RL müssen Einrichtungen im Anwendungsbereich geeignete technische, operative und organisatorische Risikomanagementmaßnahmen treffen, um Risiken zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu minimieren. Zu berücksichtigen sind dabei der Stand der Technik, einschlägige europäische und internationale Normen, die Kosten, die Risikoexposition, die Größe der Einrichtung sowie die Eintrittswahrscheinlichkeit und Schwere möglicher Vorfälle. Zu den Mindestmaßnahmen gehören unter anderem Backup-Management und Wiederherstellung nach einem Notfall, Cyberhygiene und Schulungen, Kryptografie und Verschlüsselung, Konzepte für Zugriffskontrolle und Anlagenmanagement, Multi-Faktor-Authentifizierung sowie die Sicherheit der Lieferkette.

Für Sicherheitsvorfälle sieht Art. 23 NIS-2-RL ein dreistufiges Meldemodell vor. Bei einem erheblichen Sicherheitsvorfall ist unverzüglich, spätestens innerhalb von 24 Stunden, eine Frühwarnung abzugeben; innerhalb von 72 Stunden folgt die eigentliche Meldung mit einer ersten Bewertung, und spätestens nach einem Monat ist ein detaillierter Abschlussbericht vorzulegen. Ergänzend können die Behörden einen Zwischenbericht anfordern; zudem sind potenziell betroffene Empfänger sowie soweit zur Sensibilisierung erforderlich oder im öffentlichen Interesse die Öffentlichkeit zu informieren.

5. Persönliche Verantwortung der Leitungsorgane

Von besonderer Bedeutung ist Art. 32 Abs. 6 NIS-2-RL. Danach müssen natürliche Personen, die für eine wesentliche Einrichtung verantwortlich sind oder diese vertreten, gewährleisten können, dass die Einrichtung die Vorgaben der Richtlinie erfüllt; sie können für Verstöße gegen ihre Pflichten haftbar gemacht werden. Die Folge ist eine persönliche Haftung der Führungskräfte juristischer Personen für die erweiterten Cybersicherheitspflichten und dies zusätzlich zu möglichen Geldbußen für die juristische Person selbst.

6. Umsetzungsfrist

Nach Art. 41 NIS-2-RL sollten die Mitgliedstaaten die erforderlichen Vorschriften bis zum 17. Oktober 2024 erlassen und veröffentlichen und ab dem 18. Oktober 2024 anwenden. Das deutsche Umsetzungsgesetz trat jedoch erst am 6. Dezember 2025 in Kraft und damit mit über einem Jahr Verspätung, nachdem die Europäische Kommission bereits ein Vertragsverletzungsverfahren eingeleitet hatte.

V. Die nationale Umsetzung: Das neue BSI-Gesetz

1. Das Gesetzgebungsverfahren

Der Weg zum deutschen NIS-2-Umsetzungsgesetz war langwierig. Zwischen April 2023 und Sommer 2024 durchlief das Vorhaben mehrere Referentenentwürfe, ein Diskussionspapier und ein Werkstattgespräch des Bundesministeriums des Innern sowie einen Regierungsentwurf vom 22. Juli 2024. Der Entwurf der alten Bundesregierung vom 2. Oktober 2024 wurde diskutiert, aber nicht mehr verabschiedet. Nach den Neuwahlen im Frühjahr 2025 legte die neue Bundesregierung einen ersten Regierungsentwurf (25. Juli 2025) und einen zweiten Entwurf (8. September 2025) vor. Der Bundestag verabschiedete das Gesetz am 13. November 2025, der Bundesrat stimmte zu und mit der Verkündung im Bundesgesetzblatt am 5. Dezember 2025 trat das Gesetz am 6. Dezember 2025 in Kraft ohne jede Übergangsfrist.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

2. Aufbau als Artikelgesetz

Das deutsche NIS-2-Umsetzungsgesetz ist ein Artikelgesetz: Seine verschiedenen Artikel ändern oder fassen jeweils andere Gesetze neu. Art. 1 enthält eine Neufassung des bereits bestehenden BSI-Gesetzes, das damit zum Herzstück der deutschen Umsetzung wird. Die konsolidierte Fassung des neuen BSIG ist online verfügbar (https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html).

Das Gesetz verändert die deutsche KRITIS-Regulierung deutlich. Neben die bisherigen Betreiber kritischer Anlagen treten nun „besonders wichtige“ und „wichtige“ Einrichtungen, sodass ein Mehrklassensystem von Betreibern mit unterschiedlichen Pflichtenniveaus entsteht. Die Fundstelle im Bundesgesetzblatt findet sich hier (https://www.recht.bund.de/bgbl/1/2025/301/VO).

3. Der neue Adressatenkreis (§ 28 BSIG)

Nach § 28 Abs. 1 BSIG gelten als besonders wichtige Einrichtungen zunächst die Betreiber kritischer Anlagen, qualifizierte Vertrauensdiensteanbieter, Top-Level-Domain-Registries und DNS-Dienstanbieter sowie Anbieter öffentlich zugänglicher Telekommunikationsdienste beziehungsweise Betreiber öffentlicher Telekommunikationsnetze, die mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils mehr als 10 Millionen Euro aufweisen. Als besonders wichtige Einrichtungen gelten außerdem sonstige natürliche oder juristische Personen sowie rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die entgeltlich Waren oder Dienstleistungen einer Einrichtungsart aus Anlage 1 anbieten und mindestens 250 Mitarbeiter beschäftigen oder einen Jahresumsatz von mehr als 50 Millionen Euro sowie eine Jahresbilanzsumme von mehr als 43 Millionen Euro aufweisen. Ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht zugleich Betreiber kritischer Anlagen sind.

Als wichtige Einrichtungen gelten nach § 28 Abs. 2 BSIG Vertrauensdiensteanbieter sowie Anbieter öffentlich zugänglicher Telekommunikationsdienste beziehungsweise Betreiber öffentlicher Telekommunikationsnetze mit weniger als 50 Beschäftigten und einem Jahresumsatz und einer Jahresbilanzsumme von jeweils höchstens 10 Millionen Euro. Ebenfalls als wichtige Einrichtungen gelten natürliche oder juristische Personen sowie rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die entgeltlich Waren oder Dienstleistungen einer Einrichtungsart aus Anlage 1 oder 2 anbieten und mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils mehr als 10 Millionen Euro aufweisen. Ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung.

Praktisch betroffen sind damit KRITIS-Unternehmen, besonders wichtige Einrichtungen aus einem Sektor der Anlage 1 sowie wichtige Einrichtungen aus einem Sektor der Anlage 1 oder 2 — jeweils bei entsprechender Größe beziehungsweise entsprechendem Umsatz. Die maßgeblichen Sektoren sind in den Anlagen 1 und 2 am Ende des BSIG aufgeführt (https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html). Ob ein konkretes Unternehmen erfasst ist, muss im Einzelfall geprüft werden.

Zweifel an der eigenen Betroffenheit lassen sich mithilfe der Betroffenheitsprüfung des BSI klären (https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html).

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

4. Berechnung der Schwellenwerte (§ 28 Abs. 3 und 4 BSIG)

§ 28 Abs. 3 BSIG enthält eine Bagatellklausel. Danach können bei der Zuordnung zu einer Einrichtungsart nach Anlage 1 oder 2 solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Verhältnis zur gesamten Geschäftstätigkeit der Einrichtung vernachlässigbar sind. Damit soll verhindert werden, dass eine geringfügige Nebentätigkeit zu einer unverhältnismäßigen Einstufung als wichtige oder besonders wichtige Einrichtung führt.

Für die maßgeblichen Zahlen — Mitarbeiterzahl, Jahresumsatz und Jahresbilanzsumme — gilt nach § 28 Abs. 4 BSIG grundsätzlich die KMU-Empfehlung der EU-Kommission 2003/361/EG. Bei verbundenen Unternehmen werden die Zahlen zusammengerechnet, wenn mehr als 50 % der Anteile oder Stimmrechte gehalten werden; bei Partnerunternehmen erfolgt eine Berücksichtigung ab mehr als 25 %. Eine Ausnahme kann gelten, wenn das Unternehmen hinsichtlich seiner informationstechnischen Systeme, Komponenten und Prozesse tatsächlich unabhängig ist. Hilfestellung bietet der Benutzerleitfaden der EU-Kommission zur KMU-Definition (https://op.europa.eu/de/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1/language-de).

5. Betreiber kritischer Anlagen

Die bisherigen KRITIS-Betreiber heißen nun „Betreiber kritischer Anlagen“. Die Grundsätze zur Identifikation kritischer Anlagen bleiben im Wesentlichen bestehen, die erfassten Sektoren werden jedoch leicht erweitert. Zu ihnen zählen Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungen, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum sowie Siedlungsabfallentsorgung. Betreiber kritischer Anlagen werden automatisch zu besonders wichtigen Einrichtungen im Sinne der neuen NIS-2-Systematik; für sie gelten daher zusätzlich die Pflichten dieser Gruppe. Die bisherigen KRITIS-Pflichten zu Identifikation, Registrierung, Meldung und Nachweisen bleiben im Grundsatz erhalten, werden durch die NIS-2-Umsetzung aber teilweise verändert.

VI. Die Pflichten der betroffenen Einrichtungen

Die bisherigen KRITIS-Pflichten bleiben im Grundsatz erhalten, werden aber präzisiert, verschärft und neu strukturiert. Im Überblick treffen NIS-2-Unternehmen sechs Pflichtenkomplexe: die Umsetzung von Risikomanagementmaßnahmen, die Meldung von Sicherheitsvorfällen an das BSI, die Registrierung und Identifikation beim BSI, Nachweispflichten durch Prüfung und Dokumentation, die Kommunikation mit Behörden und gegebenenfalls Betroffenen sowie Schulungspflichten für die Leitungsorgane. Betreiber kritischer Anlagen unterliegen zusätzlichen Anforderungen.

1. Risikomanagementmaßnahmen (§ 30 BSIG)

Nach § 30 Abs. 1 BSIG müssen besonders wichtige und wichtige Einrichtungen verhältnismäßige, wirksame technische und organisatorische Maßnahmen ergreifen. Diese sollen Störungen der Verfügbarkeit, Integrität und Authentizität der informationstechnischen Systeme vermeiden und die Auswirkungen von Sicherheitsvorfällen möglichst gering halten. Nach § 30 Abs. 2 Satz 1 BSIG müssen die Maßnahmen auf einem gefahrenübergreifenden Ansatz beruhen und dem Stand der Technik entsprechen.

§ 30 Abs. 2 Satz 2 BSIG benennt einen Katalog von Mindestthemen, die die Maßnahmen abdecken müssen:

- Risikoanalyse und Sicherheit für Informationssysteme;
- Bewältigung von Sicherheitsvorfällen;

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

- Aufrechterhaltung des Betriebs, etwa durch Backup-Management, Wiederherstellung nach einem Notfall und Krisenmanagement;
- Sicherheit der Lieferkette einschließlich der Beziehungen zu unmittelbaren Anbietern oder Dienstanbietern;
- Sicherheit bei Erwerb, Entwicklung und Wartung von IT-Systemen einschließlich des Schwachstellenmanagements;
- Konzepte und Verfahren zur Bewertung der Wirksamkeit der Risikomanagementmaßnahmen;
- Schulungen und Sensibilisierung im Bereich der Cybersicherheit;
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung;
- Konzepte für die Sicherheit des Personals, für die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen;
- Multi-Faktor- oder kontinuierliche Authentifizierung sowie gesicherte Sprach-, Video- und Textkommunikation und gegebenenfalls gesicherte Notfallkommunikation.

Grundlage jeder wirksamen Umsetzung ist eine strukturierte Risikoanalyse; das BSI stellt hierzu ein eigenes Infopaket bereit (https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Risikoanalyse/NIS-2-Risikoanalyse_node.html).

2. Besonderheiten für Betreiber kritischer Anlagen (§§ 31, 41 BSIG)

Betreiber kritischer Anlagen trifft ein erhöhtes Pflichtenniveau. Nach § 31 BSIG müssen sie Systeme zur Angriffserkennung einsetzen, die Bedrohungen fortwährend identifizieren und bei Störungen geeignete Beseitigungsmaßnahmen unterstützen. Nach § 41 BSIG kann das BSI zudem den Einsatz kritischer Komponenten untersagen.

3. Melde- und Unterrichtungspflichten (§§ 32, 35, 36 BSIG)

Nach § 32 BSIG müssen besonders wichtige und wichtige Einrichtungen erhebliche Sicherheitsvorfälle über die vom BSI eingerichtete Meldemöglichkeit melden. Ein Sicherheitsvorfall ist erheblich, wenn er schwerwiegende Betriebsstörungen oder finanzielle Verluste verursacht hat oder verursachen kann oder andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Die Meldung folgt einer gestuften Kaskade: Zunächst ist unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, eine frühe Erstmeldung abzugeben. Innerhalb von 72 Stunden folgt eine Bestätigung oder Aktualisierung einschließlich einer Bewertung von Schwere, Auswirkung und Kompromittierungsindikatoren. Auf Ersuchen des BSI ist eine Zwischenmeldung mit relevanten Statusaktualisierungen zu erstatten, und innerhalb eines Monats ist eine Abschluss- oder Fortschrittsmeldung mit Angaben zu Schweregrad, Art der Bedrohung, Ursache, Abhilfemaßnahmen und gegebenenfalls grenzüberschreitenden Auswirkungen vorzulegen. Betreiber kritischer Anlagen müssen zusätzlich Art und kritische Dienstleistung der betroffenen Anlage sowie die Auswirkungen des Vorfalls auf diese Anlage melden.

Nach § 35 BSIG kann das BSI bei erheblichen Sicherheitsvorfällen anordnen, dass die Einrichtung die Empfänger ihrer Dienste unverzüglich unterrichtet; Einrichtungen aus dem Finanz- und Versicherungswesen, der Informationstechnik und Telekommunikation, der IKT-Diensteverwaltung und dem Bereich digitaler Dienste müssen potenziell betroffenen Empfängern von sich aus unverzüglich geeignete Gegen- und Abhilfemaßnahmen mitteilen. Nach § 36 BSIG kann das BSI die Einrichtung zur öffentlichen Information auffordern, wenn eine Sensibilisierung der Öffentlichkeit notwendig ist.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

4. Registrierungspflicht (§ 33 BSIG)

Nach § 33 BSIG müssen sich betroffene Unternehmen spätestens drei Monate, nachdem sie erstmals oder erneut als NIS-2-Einrichtung gelten, beim BSI registrieren. Zu übermitteln sind Name, Rechtsform und gegebenenfalls Handelsregisternummer, Anschrift und aktuelle Kontaktdaten einschließlich E-Mail-Adresse, öffentlicher IP-Adressbereiche und Telefonnummer, der relevante Sektor beziehungsweise die Branche nach Anlage 1 oder 2, die EU-Mitgliedstaaten, in denen die Einrichtung Dienste erbringt, sowie die zuständigen Aufsichtsbehörden des Bundes und der Länder. Das BSI hat hierfür ein Online-Meldeportal freigeschaltet (https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Anleitung-Registrierung/Anleitung-Registrierung_node.html).

VII. Bußgeldvorschriften (§ 65 BSIG)

Das neue Recht wird durch einen umfangreichen Bußgeldkatalog flankiert. Ordnungswidrig handelt insbesondere, wer vorsätzlich oder fahrlässig Risikomanagementmaßnahmen nach § 30 BSIG nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig umsetzt, die Maßnahmen nicht ordnungsgemäß dokumentiert, Melde- oder Registrierungspflichten verletzt, vollziehbaren Anordnungen zuwiderhandelt, über die angegebene Kontaktstelle nicht erreichbar ist, erforderliche Zugänge oder Nachweise nicht rechtzeitig gewährt oder unberechtigt vorgibt, Inhaber einer Zertifizierung zu sein. Nahezu jede Nichterfüllung einer gesetzlichen Pflicht kann damit mit einem Bußgeld belegt werden.

Die Höhe der Bußgelder ist nach § 65 Abs. 5 bis 7 BSIG gestaffelt; bei bestimmten Verstößen können bis zu 2 % des weltweiten Jahresumsatzes angesetzt werden. Der Rahmen im Überblick:

Verstoß / Einrichtung	Bußgeldrahmen
Besonders wichtige Einrichtungen	bis 10 Mio. € oder 2 % des weltweiten Jahresumsatzes
Wichtige Einrichtungen	bis 7 Mio. € oder 1,4 % des weltweiten Jahresumsatzes
Verstoß gegen die Registrierungspflicht	bis 500.000 €, unabhängig vom Umsatz

Maßgeblich ist jeweils der höhere Betrag. Zu beachten ist, dass Nachweisverstöße nach § 65 Abs. 1 BSIG ausschließlich Betreiber kritischer Anlagen treffen, nicht alle besonders wichtigen Einrichtungen. Bei Verstößen mit Bezug zu personenbezogenen Daten können zusätzlich Bußgelder nach der DS-GVO hinzutreten. Praktisch besonders relevant sind die fehlende Registrierung, nicht dokumentierte Risikomanagementmaßnahmen und versäumte Meldungen.

Neben dem Bußgeld gegen die Einrichtung besteht die Binnenhaftung der Geschäftsleitung nach § 38 Abs. 2 BSIG in Verbindung mit dem Gesellschaftsrecht, insbesondere § 93 AktG und § 43 Abs. 2 GmbHG. Der entscheidende Merksatz lautet: Das Bußgeld trifft die Einrichtung, die Binnenhaftung trifft die Person.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

VIII. Haftung und Schulungspflichten der Geschäftsleitung (§ 38 BSIG)

1. Sinn und Zweck der Geschäftsleitungshaftung

Mit der Umsetzung der NIS-2-Richtlinie steigen die Anforderungen an Unternehmen, Cybersicherheitsmaßnahmen systematisch zu planen, umzusetzen und zu überwachen. Die Geschäftsleitung muss gewährleisten, dass Cybersicherheit integraler Bestandteil der Unternehmensgeschäfte ist, in das Risikomanagement eingebunden wird und durch geeignete Maßnahmen tatsächlich umgesetzt und überwacht wird. Diese besondere Verantwortung und die Schulungspflicht der Geschäftsleitung sind gesetzlich vorgeschrieben.

§ 38 BSIG setzt Art. 20 NIS-2-RL um und konkretisiert die Pflichten organschaftlicher Geschäftsleitungen. Nach der Stellungnahme des Gesetzgebers muss die Geschäftsleitung dafür sorgen, dass die erforderlichen Maßnahmen tatsächlich umgesetzt und kontinuierlich überwacht werden. Hilfspersonen können eingeschaltet werden; das Leitungsorgan bleibt jedoch letztverantwortlich. Die Bedeutung der Geschäftsleitungshaftung liegt damit in drei Aspekten: der Verantwortungsübernahme für angemessene Cybersicherheitsstrategien, der Rechenschaftspflicht bei unzureichender Umsetzung und der Förderung einer Unternehmenskultur, die angemessene Sicherheitspraktiken auf höchster Ebene unterstützt und durchsetzt.

2. Umsetzungs- und Überwachungspflicht (§ 38 Abs. 1 BSIG)

Nach § 38 Abs. 1 BSIG müssen die Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen die Risikomanagementmaßnahmen nach § 30 umsetzen und deren Umsetzung überwachen. Die Verantwortung erschöpft sich also nicht in einer einmaligen Einführung von Maßnahmen, sondern umfasst deren fortlaufende Kontrolle.

3. Binnenhaftung bei Pflichtverletzungen (§ 38 Abs. 2 BSIG)

Nach § 38 Abs. 2 BSIG haften Geschäftsleitungen bei schuldhafter Pflichtverletzung gegenüber ihrer Einrichtung nach den auf die jeweilige Rechtsform anwendbaren Regeln des Gesellschaftsrechts. Die Binnenhaftung folgt damit grundsätzlich den allgemeinen gesellschaftsrechtlichen Regeln, insbesondere § 93 AktG und § 43 Abs. 2 GmbHG. Anders als das Bußgeld, das die juristische Person trifft, richtet sich diese Haftung unmittelbar gegen die verantwortliche natürliche Person.

4. Schulungspflicht (§ 38 Abs. 3 BSIG)

Nach § 38 Abs. 3 BSIG müssen Geschäftsleitungen regelmäßig an Schulungen teilnehmen. Ziel ist der Erwerb von Kenntnissen und Fähigkeiten, um Risiken und Risikomanagementpraktiken im Bereich der Informationssicherheit zu erkennen und zu bewerten sowie deren Auswirkungen auf die von der Einrichtung erbrachten Dienste beurteilen zu können. Leitungen von Einrichtungen der Bundesverwaltung gelten dabei nicht als Geschäftsleitung im Sinne der Vorschrift. Das BSI hat zur Ausgestaltung der Schulungspflicht ein eigenes Infopaket veröffentlicht (https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Geschaeftsleitungsschulung/NIS-2-Geschaeftsleitungsschulung_node.html).

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

5. Delegation und Nachweis

Die persönliche Haftung der Geschäftsleitung lässt sich nicht vollständig delegieren. Einzelne Aufgaben können jedoch wirksam an einen Chief Information Security Officer (CISO) oder die IT-Leitung übertragen werden, wenn Verantwortlichkeiten, Prozesse und Reporting klar geregelt sind. Durch ein dokumentiertes Reporting kann die Erfüllung der Risikomanagement- und Meldepflichten nachgewiesen werden. Das BSI unterstützt die Umsetzung mit einer Betroffenheitsprüfung, einem Starterpaket und weiteren Hilfsmitteln (https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-was-tun/NIS-2-was-tun.html).

IX. Fristen und praktische Umsetzung

Für die Praxis ist eine Reihe von Fristen maßgeblich. Das deutsche NIS-2-Umsetzungsgesetz gilt seit dem 6. Dezember 2025. Die Registrierung als wichtige oder besonders wichtige Einrichtung musste nach der gesetzlichen Frist des § 33 Abs. 1 BSIG bis zum 6. März 2026 über das BSI-Portal erfolgen. Änderungen der Registrierungsangaben sind innerhalb von zwei Wochen nach der tatsächlichen Änderung mitzuteilen. Erste Nachweisprüfungen werden voraussichtlich frühestens ab dem Winter 2028/2029 stattfinden.

Zum gesetzlichen Fristablauf am 6. März 2026 waren von den rund 29.500 betroffenen Einrichtungen in Deutschland erst etwa 11.500 registriert; bis Ende Mai 2026 stieg die Zahl auf rund 18.500. Vor diesem Hintergrund hat das BSI eine Nachfrist bis zum 31. Juli 2026 gewährt. Dabei handelt es sich allerdings nur um eine behördliche Duldung, nicht um eine echte Fristverlängerung: Eine verspätete Registrierung bleibt eine Ordnungswidrigkeit und kann nach § 65 BSIG mit bis zu 500.000 Euro geahndet werden. Nach dem 31. Juli 2026 ist mit einer konsequenteren Überwachung zu rechnen.

In der praktischen Abfolge ist zu beachten, dass zunächst das ELSTER-Organisationszertifikat über „Mein Unternehmenskonto“ beantragt werden muss; erst danach ist die Registrierung im BSI-Portal möglich. Wer Zweifel an der eigenen Betroffenheit hat, kann diese beim BSI prüfen lassen; nach der Antwort läuft eine weitere Frist von sechs Wochen. Die einschlägigen Hilfsmittel und die Anleitung zur Registrierung stellt das BSI bereit (https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Anleitung-Registrierung/Anleitung-Registrierung_node.html).

X. Flankierende Regelungen aus Brüssel und Berlin

Das NIS-2-Umsetzungsgesetz steht nicht für sich allein. Es wird durch weitere europäische und nationale Regelungen ergänzt, die für viele Unternehmen parallel gelten und den Rahmen der Cybersicherheits-Compliance in den kommenden Jahren wesentlich prägen.

1. Das KRITIS-Dachgesetz

Das KRITIS-Dachgesetz ist seit dem 17. März 2026 in Kraft. Der Bundestag beschloss das Gesetz am 29. Januar 2026, der Bundesrat stimmte am 6. März 2026 zu, die Verkündung im Bundesgesetzblatt erfolgte am 11. März 2026. Das Gesetz setzt die CER-Richtlinie (EU) 2022/2557 um und schafft erstmals bundeseinheitliche Mindeststandards für die physische Sicherheit kritischer Anlagen. Es verlangt unter anderem Resilienzpläne, eine Risikobewertung, Objekt- und Perimeterschutz sowie ein Krisenmanagement. Betroffen sind rund 2.000 Betreiber in elf Sektoren.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Für die Beratungspraxis sind vier Punkte zentral: Zuständig ist das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), nicht das BSI. Die Registrierungsfrist lief bereits am 17. Juli 2026 ab. Für bestimmte Betreiber besteht nach § 39 Abs. 4 BSIG keine Nachweispflicht. Und schließlich ist die Doppelbetroffenheit der Regelfall: NIS-2 schützt die IT, das KRITIS-Dachgesetz die Anlage. Die beiden Regime im Vergleich:

	NIS-2 / BSIG	KRITIS-Dachgesetz
Rechtsgrundlage	RL (EU) 2022/2555 → BSIG, in Kraft seit 06.12.2025	RL (EU) 2022/2557 → KRITIS-DachG, in Kraft seit 17.03.2026
Schutzrichtung	Cyber- und Informationssicherheit	Physische Resilienz, All-Gefahren-Ansatz
Adressaten	Besonders wichtige und wichtige Einrichtungen (rund 29.500)	Betreiber kritischer Anlagen (rund 2.000)
Aufsicht	BSI	BBK
Registrierung	BSI-Portal, § 33 BSIG; Duldung bis 31.07.2026	BBK; Frist am 17.07.2026 abgelaufen
Kernpflichten	§ 30 Risikomanagement, § 32 Meldung, § 38 Geschäftsleitung	Resilienzplan, Risikobewertung, Objektschutz, Meldepflichten

2. Die Durchführungsverordnung (EU) 2024/2690

Für bestimmte digitale Dienste und Infrastrukturen gilt die Durchführungsverordnung (EU) 2024/2690. Sie ist unmittelbar verbindlich unter anderem für DNS-Diensteanbieter und TLD-Registries, Cloud-Computing- und Rechenzentrumsdienste, Content Delivery Networks, Managed (Security) Service Provider, Online-Marktplätze, Online-Suchmaschinen und Plattformen sozialer Netzwerke sowie Vertrauensdiensteanbieter. Die darin konkretisierten Risikomanagementmaßnahmen mussten grundsätzlich bereits seit Oktober 2024 umgesetzt sein; nähere Informationen stellt die Europäische Kommission bereit (https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks).

Die Bedeutung der Verordnung reicht über ihren unmittelbaren Adressatenkreis hinaus. Sie gilt seit dem 18. Oktober 2024 ohne nationale Umsetzung und konkretisiert die zehn Maßnahmenbereiche technisch — von der Zugriffskontrolle bis zum Schwachstellenmanagement. Faktisch wird sie europaweit als Auslegungsmaßstab für Art. 21 NIS-2-RL beziehungsweise § 30 BSIG herangezogen; Aufsichtsbehörden, Auditoren und Kunden in der Lieferkette orientieren sich an ihr. Es empfiehlt sich daher, die Gap-Analyse gegen den Anhang der Durchführungsverordnung zu führen und nicht nur gegen den Wortlaut des § 30 BSIG.

3. Der Cyber Resilience Act

Eine weitere Regelungswelle bringt der Cyber Resilience Act (Verordnung (EU) 2024/2847), der im Dezember 2024 in Kraft getreten ist. Ab dem 11. September 2026 greifen die Meldepflichten für Hersteller; die vollständige Anwendung aller Produktanforderungen folgt am 11. Dezember 2027. Die Meldekaskade ab September 2026 sieht bei aktiv ausgenutzten Schwachstellen und schwerwiegenden Sicherheitsvorfällen eine Frühwarnung innerhalb von 24 Stunden, weitere Informationen innerhalb von 72 Stunden sowie einen Abschlussbericht vor: bei Schwachstellen 14 Tage nach dem Sicherheitsupdate, bei Vorfällen einen Monat nach der Erstmeldung.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Für die NIS-2-Compliance ist der Cyber Resilience Act unmittelbar relevant, weil er Produkte mit digitalen Elementen erfasst und ab September 2026 auch das Bestandsportfolio reguliert. Es besteht eine direkte Schnittstelle zu § 30 Abs. 2 Nr. 4 und 5 BSIG, also zur Lieferkettensicherheit sowie zu Erwerb, Entwicklung, Wartung und Schwachstellenmanagement. Der Bußgeldrahmen reicht bis 15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes.

XI. Fazit und Ausblick

Die NIS-2-Richtlinie und ihre deutsche Umsetzung markieren einen Paradigmenwechsel im Recht der IT-Sicherheit. Die Richtlinie gibt die wesentlichen Pflichten zur Cybersicherheit, die Meldepflichten und die Haftung der Geschäftsleitung bereits vor; der deutsche Gesetzgeber hat diese Inhalte mit dem neu gefassten BSI-Gesetz in nationales Recht überführt. Der Kreis der verpflichteten Unternehmen ist dadurch von rund 1.600 auf etwa 30.000 Einrichtungen angewachsen.

Im Zentrum steht die persönliche Verantwortung der Unternehmensleitung. Die Geschäftsleitung muss die Risikomanagementmaßnahmen umsetzen und überwachen. Sie haftet bei schuldhafter Pflichtverletzung nach gesellschaftsrechtlichen Regeln persönlich und sie muss regelmäßig an Schulungen teilnehmen. Eine vollständige Delegation der Haftung ist nicht möglich, gleichwohl lassen sich Aufgaben wirksam übertragen, wenn Verantwortlichkeiten, Prozesse und ein dokumentiertes Reporting klar geregelt sind.

Für die Praxis bedeutet dies: Cybersicherheit wird erstens zu einer dauerhaften Compliance-Aufgabe und die Nachfrage nach entsprechender Expertise wird zweitens binnen kurzer Zeit stark ansteigen. Unternehmen, die das neue BSIG, das KRITIS-Dachgesetz, die Durchführungsverordnung (EU) 2024/2690 und den Cyber Resilience Act zusammen denken und ihre Maßnahmen an den konkretisierenden europäischen Vorgaben ausrichten, sind für die kommenden Prüfungszyklen am besten aufgestellt.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Seminartipps zum Arbeitspapier

IT-Sicherheitsmanagement aus Sicht des/der Datenschutzbeauftragten

Die DS-GVO regelt auch den Einsatz von IT-Produkten, IT-Sicherheitsmaßnahmen und ihre Dokumentation. Z. B. sind deren Einsatz oder auch Verzicht – wie für andere technische und organisatorische Maßnahmen auch – mittels einer Risikoanalyse zu begründen und die Angemessenheit nachzuweisen. Datenschutzbeauftragte, Datenschutzfachkräfte und Compliance Manager stehen deshalb vor der Herausforderung, die rechtliche Zulässigkeit von technischen Maßnahmen, Geräten und Dienstleistungen zu beurteilen, mitzugestalten und zu prüfen. Als Datenschutzprofis sind sie die ersten Ansprechpartner für Unternehmensführung und IT-Fachkräfte. Dabei stehen Unternehmen unabhängig von ihrer Größe vor den gleichen Herausforderungen.

Durch die drastisch erhöhten Bußgelder, auf 10 Mio. Euro und mehr, die auch bei vermeintlich harmlosen Bagatellverstößen verhängt werden können, kann die Missachtung von datenschutzrechtlichen Vorschriften gravierende Folgen für die Unternehmen haben.

Weitere Infos finden Sie hier.

Gorodenkoff | Bernulius - stock.adobe.com

Basiswissen IT-Sicherheit für Datenschutzbeauftragte & -Manager

Dieses praxisnahe Seminar gibt Ihnen einen einsteigerfreundlichen Überblick über die wichtigsten Begriffe, Funktionen und Technologien der IT-Sicherheit. Sie erfahren, wie Datenschutz, IT-Sicherheit, Informationssicherheit und Risikomanagement im Unternehmen zusammenwirken und sich gegenseitig stärken können.

Anhand typischer Bedrohungen aus der Praxis – etwa DDoS-Angriffen, Phishing, Ransomware, Botnets oder unsicheren Passwörtern – sowie grundlegender Schutzmechanismen wie Firewalls, VPN, Multi-Faktor-Authentifizierung, Verschlüsselung und einfachen Backup-Strategien lernen Sie, wie sich digitale Risiken erkennen und die eigene Angriffsfläche wirksam reduzieren lassen.

Anschauliche Beispiele verdeutlichen, wie KI moderne Schutzmaßnahmen wie Anomalieerkennung unterstützt, zugleich aber – etwa durch KI-basierte Re-Personalisierung vermeintlich anonymer Daten in Kombination mit Big Data-Analysen – neue personalisierte Cyberangriffe entstehen, die auch den Datenschutz erheblich herausfordern.

Weitere Infos finden Sie hier.

Elva - stock.adobe.com

DataAgenda
ist das Lösungsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet News, Tools und Tipps rund um den Datenschutz.

Datakontext
ist einer der führenden Fachinformationsdienstleister in den Bereichen Datenschutz und IT-Sicherheit und bietet Kompetenz aus einer Hand: Fachbücher, Fachzeitschriften und Seminare, Zertifizierung und Beratung.

Autoren

Prof. Dr. Rolf Schwartmann
Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V (GDD), Leiter der Kölner Forschungsstelle für Medienrecht (TH Köln) und Mitglied der Datenethikkommission.

Dr. Tobias Jacquemain, LL.M. (GDD e.V.)
Promotion zum Schadensersatz für Datenschutzverstöße nach Art. 82 DS-GVO und Lehrbeauftragter an der Universität zu Köln, an der Technischen Hochschule (TH) Köln sowie an der TH Georg Agricola in Bochum.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com