DataAgenda-Arbeitspapier 80, 2/2026

DataAgenda - das Informationsportal zum Datenschutzrecht

Präsentiert von DATAKONTEXT

www.DataAgenda.de

Die NIS2-Umsetzung

Ein Arbeitspapier zur Reform des deutschen Cybersicherheitsrechts

I. Einleitung

Mit dem Inkrafttreten des Gesetzes zur Umsetzung der NIS-2-Richtlinie am 6. Dezember 2025 wurde das deutsche Cybersicherheitsrecht umfassend modernisiert. Ziel der Reform ist es, die Resilienz und Widerstandsfähigkeit digitaler Infrastrukturen europaweit zu erhöhen. Rund 30.000 Unternehmen und Organisationen in Deutschland fallen künftig unter den erweiterten Anwendungsbereich des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die NIS2-Umsetzung stellt den größten regulatorischen Eingriff in die Cybersicherheits-Governance seit Einführung des IT-Sicherheitsgesetzes dar. Dieses Arbeitspapier analysiert Zielsetzung, Anwendungsbereich und Pflichten des Gesetzes sowie die praktischen Handlungsanforderungen für betroffene Unternehmen.

II. Hintergrund und Zielsetzung der NIS2-Richtlinie

Die NIS-2-Richtlinie (EU) 2022/2555 ersetzt die bisherige NIS-Richtlinie von 2016. Sie verfolgt das Ziel, ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Europäischen Union (EU) sicherzustellen. Dabei rückt sie die Verantwortung der Geschäftsleitung, die Einbindung der gesamten Lieferkette und ein kohärentes Meldewesen in den Fokus.

Deutschland hat die Richtlinie im Dezember 2025 mit dem „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ in nationales Recht überführt. Kernstück der Umsetzung ist die Anpassung und Ausweitung des BSI-Gesetzes (BSIG).

III. Betroffene Akteure

1. Kategorien betroffener Einrichtungen

Das Gesetz unterscheidet zwischen:

- **Besonders wichtigen Einrichtungen (§ 28 BSIG-neu)**
  Darunter fallen Betreiber kritischer Anlagen, qualifizierte Vertrauensdiensteanbieter, Betreiber von Top-Level-Domains, DNS- und Telekommunikationsanbietern sowie Unternehmen bestimmter Wirtschaftszweige, die über definierte Beschäftigten- oder Umsatzgrenzen hinausgehen (in der Regel mehr als 250 Beschäftigte bzw. Umsatz oberhalb von EUR 50 Mio.).
- **Wichtige Einrichtungen**
  Hierzu zählen kleinere Betreiber aus den gleichen Sektoren, die jedoch Schwellenwerte von 50 Beschäftigten bzw. einem Umsatz von > 10 Mio. € überschreiten.

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

- **Betreiber kritischer Anlagen (KRITIS)**
  Betreiber kritischer Anlagen werden weiterhin nach sektorenspezifischen Schwellenwerten bewertet. Grundlage bleibt die etablierte KRITIS-Methodik, die im Zuge des neuen KRITIS-Dachgesetzes integriert wird.
- **Einrichtungen der Bundesverwaltung**
  In Ausnahmefällen können auch Bundesbehörden einbezogen werden, etwa wenn sie sicherheitsrelevante Infrastrukturen betreiben.

2. Ausnahmen

Teilbereiche können ausgenommen werden, wenn ihr Anteil am Gesamtgeschäft „vernachlässigbar" ist. Diese Ausnahmeregel erfordert eine nachvollziehbare Risiko- und Relevanzbewertung durch das Unternehmen.

IV. Pflichten der betroffenen Einrichtungen

1. Informationssicherheits- und Risikomanagement

Alle betroffenen Unternehmen müssen ein systematisches **Risikomanagementsystem** für Informationssicherheit etablieren. Dieses umfasst die Identifikation, Bewertung und Behandlung von Risiken sowie die Implementierung geeigneter technischer und organisatorischer Maßnahmen (TOMs).

Zu den zentralen Anforderungen zählen:

- Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach anerkannten Standards (z. B. ISO/IEC 27001 oder BSI-Grundschutz);
- Gewährleistung von Backup-, Wiederherstellungs- und Notfallmanagement;
- Implementierung von Verfahren zur kontinuierlichen Risikoanalyse und -bewertung;
- Nachweis der Sicherheit über den gesamten Systemlebenszyklus (Entwicklung, Beschaffung, Wartung).

2. Meldepflichten und Incident Response

Einrichtungen müssen erhebliche Sicherheitsvorfälle zeitnah an das BSI melden. Dies setzt etablierte Prozesse innerhalb der Einrichtungen voraus. Der Prozess umfasst die Phasen:

1. Früherkennung und Bewertung des Vorfalls
2. Erstmeldung an das BSI (innerhalb von 24 Stunden nach Feststellung)
3. Zwischenbericht mit vorläufiger Analyse
4. Abschlussmeldung mit detaillierter Ursachenbewertung und Gegenmaßnahmen

3. Lieferkettensicherheit

Ein bedeutender neuer Aspekt ist der Fokus auf **Cybersicherheit in der Lieferkette**. Unternehmen sind verpflichtet, sicherzustellen, dass auch beauftragte Dritte – insbesondere IT-Dienstleister, Cloud-Anbieter und Zulieferer – ein angemessenes Sicherheitsniveau wahren. Dies kann durch vertragliche Verpflichtungen, Audits oder Zertifizierungen erfolgen.

4. Verantwortung der Unternehmensleitung

Nach § 38 BSIG-neu übernimmt die Geschäftsleitung persönlich Verantwortung für die Umsetzung der Sicherheitsmaßnahmen. Dazu gehört:

- Einrichtung und Überwachung des ISMS;
- Genehmigung der Cybersicherheitsstrategie;

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

- Teilnahme an verpflichtenden Schulungen;
- Haftungsrechtliche Verantwortung bei Pflichtverstößen.

Diese Regelung verdeutlicht den Wandel von IT-Sicherheit als technischem Thema hin zu einer **strategischen Führungsaufgabe**.

V. Registrierungspflichten und organisatorische Umstellung

1. Zweistufiges Registrierungsverfahren

Betroffene Organisationen müssen sich nach folgendem Verfahren beim BSI registrieren:

1. **Registrierung beim Dienst „Mein Unternehmenskonto“ (MUK)**

   Das MUK ist das OZG-konforme Nutzerkonto für juristische Personen und schafft den Zugang zu staatlichen Online-Verwaltungsleistungen.

2. **Registrierung im neuen BSI-Portal**

   Ab dem 6. Januar 2026 wird das Portal freigeschaltet und fungiert als zentrale Anlaufstelle für Meldungen, Registrierungen und Austausch mit dem BSI.

Bei Sicherheitsvorfällen vor der Registrierung steht ein temporäres Online-Formular zur Verfügung. KRITIS-Betreiber bleiben bis zur vollständigen Systemumstellung bei ihren bisherigen Meldewegen.

2. Übergangs- und Handlungsempfehlungen

Unternehmen sollten:

- den MUK-Account spätestens bis Ende 2025 anlegen,
- interne Zuständigkeiten für BSI-Kommunikation festlegen,
- bereits vorab Meldeprozesse und Schwellenwerte definieren,
- Verantwortlichkeiten im ISMS klar dokumentieren.

VI. Sanktionen und Durchsetzung

Die NIS2-Umsetzung sieht deutlich schärfere Bußgeldtatbestände vor. Verstöße gegen Melde-, Sicherheits- oder Registrierungspflichten können für besonders wichtige Einrichtungen mit bis zu **10 Mio. € oder 2 % des weltweiten Jahresumsatzes** sanktioniert werden (§ 65 BSIG-neu).

Darüber hinaus kann das BSI Aufsichtsmaßnahmen verhängen, wie etwa Anordnungen von Audits, Sicherheitsprüfungen oder die Bestellung externer Prüfer. Die Öffentlichkeit kann über erhebliche Verstöße informiert werden, was ein erhebliches Reputationsrisiko erzeugt.

VII. Fazit und Ausblick

Mit der NIS2-Umsetzung tritt Deutschland in eine neue Phase der Cybersicherheitsregulierung ein. Der gesetzliche Rahmen ist klar auf Prävention, Resilienz und Verantwortlichkeit ausgerichtet. Zahlreiche Unternehmen, die bislang nicht reguliert waren, müssen nun umfassende Sicherheitsstrukturen etablieren und vorhalten.

Der Erfolg der Reform hängt wesentlich davon ab, ob Unternehmen die Anforderungen nicht als reine Compliance-Anforderung umsetzen, sondern die zusätzliche Regulierung im besten Fall als Chance für strategische Sicherheitsmodernisierung verstehen. Cyber- und Informationssicherheit werden damit zu einem integralen Bestandteil der Unternehmensführung und zu einem entscheidenden Wettbewerbsfaktor in der (digitalen) Wirtschaft.

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

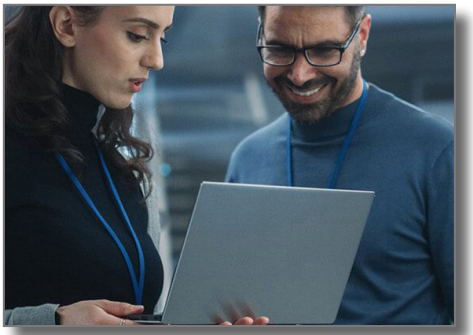
Seminartipp zum Arbeitspapier

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

DataAgenda
ist das Informationsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet Videos, News, Whitepaper und Seminartipps 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.