2026 CAMPUS TAGE

DSN Akademie

10 Jahre DSGVO

Und jetzt?
Gemeinsam weiterdenken!

DSN Akademie

NIS-2 und ihre Auswirkungen auf die Praxis

Bedeutung des Gesetzes für Unternehmen und ihre Lieferketten

www.dsn-group.de

DSN Akademie

Thomas Wennemann
Prokurist | Leiter Informationssicherheit

datenschutz nord GmbH
T +49 (0)421 69 66 32 346
E-Mail twennemann@datenschutz-nord.de

www.dsn-group.de

DSN Akademie

Organisationen, die sich bisher nicht mit Informationssicherheit auseinandergesetzt haben, setzen sich jetzt mit Informationssicherheit auseinander.

Wesentliche Fragen

Das sollte sich jedes Unternehmen beantworten können!

1. **Sind wir betroffen?**
   Selbstidentifikation in 18 Sektoren - der Staat sagt es Ihnen nicht.
2. **Wer hat unsere Sicherheitsmaßnahmen freigegeben?**
   § 38 BSIG verlangt Umsetzung und Überwachung durch die Geschäftsleitung — nicht durch die IT.
3. **Was passiert bei einem Vorfall?**
   24 Stunden, 72 Stunden, ein Monat.
4. **Was fordern unsere Kund*innen?**
   Regulierte Organisationen geben Pflichten weiter - per Vertrag und Fragebogen.

Wichtige Termine

Verstrichene Frist und noch anstehender Termin

1. 06.12.2025
   Inkrafttreten
   Neues BSIG. Keine Übergangsfrist – alle Pflichten gelten sofort.
2. 06.03.2026
   Gesetzliche Frist
   Registrierungsfrist nach § 33 BSIG. Nur etwa ein Drittel meldete sich rechtzeitig.
3. 31.07.2026
   Erste Erwartung
   Vom BSI gegenüber den Verbänden kommunizierte Erwartung – keine Fristverlängerung.
4. 30.09.2026
   Aktuelle Ansage
   Für Registrierungen, die wegen offener Auslegungsfragen ausstanden.

BEACHTE: Die gesetzliche Frist war der 6. März 2026 - alles danach ist Vollstreckungsermessen!

KRITIS-Nische

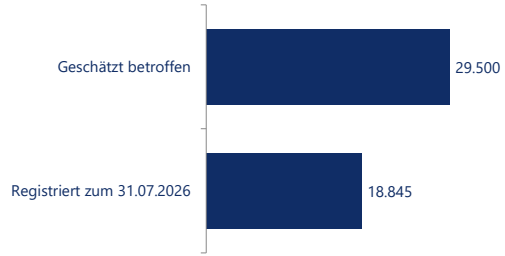
Aus der KRITIS-Nische in den Mittelstand!

ca. 4.500	ca. 29.500	18	0
Einrichtungen waren zuvor KRITIS-reguliert	Einrichtungen sollen nun unter NIS-2 fallen	Sektoren nach Anlage 1 und Anlage 2	Tage Übergangsfrist ab Inkrafttreten

BEACHTE: *NIS-2 trifft überwiegend Organisationen, die noch nie mit dem BSI zu tun hatten. Die Breite entsteht nicht über den Anwendungsbereich, sondern über die Lieferkette.*

Anzahl betroffener Unternehmen

Konkrete Zahlen unbekannt!



- Der Staat teilt die Betroffenheit nicht mit - jedes Unternehmen muss sie selbst feststellen (§ 28 BSIG).
- Die Sektorzuordnung ist bei Mischbetrieben und Dienstleistern nicht eindeutig. Das BSI hat seine FAQ dazu erweitert.

Einordnung

Zwei Klassen, zwei Schwellen - und viele Grenzfälle

§ 28 Abs. 1 BSIG
Besonders wichtige Einrichtungen

- Sektoren der Anlage 1 (hohe Kritikalität)
- ab 250 Beschäftigten oder
- über 50 Mio. € Umsatz und über 43 Mio. € Bilanzsumme
- Zusätzliche Ausnahmen unabhängig von der Größe

§ 28 Abs. 2 BSIG
Wichtige Einrichtungen

- Sektoren der Anlage 1 und der Anlage 2
- ab 50 Beschäftigten oder
- über 10 Mio. € Umsatz und über 10 Mio. € Bilanzsumme
- Zusätzliche Ausnahmen unabhängig von der Größe

BEACHTE: ***Die Sektorfrage ist meist schnell beantwortet. Die Zweifelsfälle liegen bei Konzernzurechnung, Mischbetrieben und konzerninterner IT.***

Prüfung

Die Betroffenheitsprüfung ist ein Compliance-Dokument

Was schiefgehen kann:

- Betroffenheit wird mündlich „geklärt" und nie dokumentiert
- Die Prüfung endet beim Mutterkonzern, obwohl Tochtergesellschaften eigenständig betroffen sind
- Ein negatives Ergebnis wird nicht begründet – und hält damit weder im Lieferantenfragebogen noch gegenüber dem BSI stand
- Die Registrierung im BSI-Portal wird für die Prüfung gehalten – das Formular erfasst die Konzernzurechnung nicht

Was hilft:

- Betroffenheitsanalyse als schriftliches Prüfergebnis, mit Datum und Verantwortlichem
- Auch das Ergebnis „nicht betroffen" dokumentieren und nachhalten
- Änderungsanlässe definieren: Zukäufe, Umsatzsprünge, neue Geschäftsfelder, neue Sektoren

BEACHTE: ***Die Aufsicht wird nicht fragen, ob Sie betroffen sind. Sie wird fragen, wie Sie zu Ihrem Ergebnis gekommen sind.***

Adressat

Umsetzen, überwachen, schulen – und wer dafür haftet

1 Umsetzen
Die Maßnahmen nach § 30 sind von der Geschäftsleitung umzusetzen – nicht nur zur Kenntnis zu nehmen.

2 Überwachen
Die Umsetzung ist laufend zu überwachen.

3 Schulen
Regelmäßige Schulung der Leitungsebene zu Cybersicherheit und Risikomanagement.

BEACHTE: ***§ 38 Abs. 2 begründet keine neue Haftung, sondern verweist auf das Gesellschaftsrecht der jeweiligen Rechtsform.***

Meldekaskade

Die Fristen sind einfach. Die Organisation ist es nicht.

1 24 Stunden
Erstmeldung
Frühwarnung an das BSI: erster Verdacht, Art des Vorfalls, mögliche grenzüberschreitende Auswirkungen.

2 72 Stunden
Aktualisierung
Bewertung, Schwere, Auswirkungen und Indikatoren für eine Kompromittierung.

3 1 Monat nach der 2. Meldung
Abschlussmeldung
Ursachenanalyse, ergriffene Maßnahmen, grenzüberschreitende Folgen.

Fragen, die sich in der Praxis ergeben
Wessen Kenntnis löst die 24-Stunden-Frist aus — bspw. die des SOC, eines Dienstleisters oder der Geschäftsleitung? Wer darf die Meldung freigeben, wenn die Leitung nicht erreichbar ist? Wer kann melden? Wer entscheidet gleichzeitig über die DSGVO-Meldung?

Vorfall

Drei Meldewege – drei verschiedene Logiken

§ 32 BSIG
NIS-2-Meldung

- Schutzgut: Verfügbarkeit und Integrität der Dienste
- Auslöser: erheblicher Sicherheitsvorfall
- Adressat: BSI als gemeinsame Meldestelle
- Takt: 24 Stunden, 72 Stunden, ein Monat

Art. 33 DSGVO
Datenschutzmeldung

- Schutzgut: Rechte betroffener Personen
- Auslöser: Verletzung des Schutzes personenbezogener Daten
- Adressat: Datenschutzaufsichtsbehörde, ggf. Benachrichtigung der Betroffenen
- Takt: 72 Stunden

Artikel 14 CRA – ab 11.09.2026
Schwachstellenmeldung

- Schutzgut: Sicherheit der Produkte am Markt
- Auslöser: aktiv ausgenutzte Schwachstelle oder schwerer Vorfall
- Adressat: ENISA und BSI als nationales CSIRT, ggf. Benachrichtigung der Nutzer
- Takt: 24 und 72 Stunden, 14 Tage

Konsequenz für die Organisation
Ein Vorfallsprozess, eine Faktenbasis, drei Ausgänge. Zwei der drei Meldungen landen beim BSI – über verschiedene Portale und Rechtsgrundlagen. Wer sie getrennt aufbaut, liefert ggfs. widersprüchliche Angaben.

Lieferkette

Der größte Hebel

Schätzungsweise 29.500 Einrichtungen sind reguliert. Die Anforderungen erreichen auch ihre Zulieferer.

Lieferkettensicherheit ist einer der Maßnahmenbereiche des § 30 BSIG. Regulierte Einrichtungen können ihre Pflichten nicht erfüllen, ohne Anforderungen weiterzugeben – vertraglich, über Fragebögen, über Prüfrechte.

Deshalb ist „nicht betroffen" keine Entwarnung, sondern eine Vertriebsfrage: Wer die Anforderungen seiner Kunden nicht beantworten kann, verliert Aufträge - lange bevor eine Behörde fragt.

1 **Vertrag**
NIS-2-Klauseln neben dem AV-Vertrag: Sicherheitsniveau, Meldepflichten, Unterauftragnehmer.

2 **Nachweis**
Zertifikate, Prüfberichte, Fragebögen.

3 **Prüfrechte**
Umfang, Häufigkeit und Grenzen von Audits.

Nachweise

Wirksamkeit statt Aktenlage

Wer muss aktiv nachweisen?

- Betreiber kritischer Anlagen: Nachweis gegenüber dem BSI alle drei Jahre (§ 39 BSIG).
- Alle anderen: keine turnusmäßige Vorlage, aber Stichproben, Auskunfts- und Nachweisverlangen.
- Faktisch derselbe Reifegrad – nur ohne festen Termin, an dem man fertig sein muss.

ISO/IEC 27001
Skalierbar in der Tiefe. In Lieferketten anerkannt.

BSI IT-Grundschutz
Modular und begrifflich anschlussfähig, aber aufwändig.

Branchenstandard (§ 30 Abs. 8 BSIG)
Vom Verband vorgeschlagen, vom BSI geprüft und veröffentlicht.

Eigenlösung
Zulässig, aber Wirksamkeit und Angemessenheit sind selbst zu belegen.

BEACHTE: § 30 Abs. 2 BSIG verlangt den Stand der Technik und die Berücksichtigung europäischer und internationaler Normen – kein bestimmtes Rahmenwerk und kein Zertifikat.

Bußgeldrahmen

Hoher Rahmen, keine bekannte Praxis

BESONDERS WICHTIGE EINRICHTUNGEN
bis 10 Mio. €
oder bis 2 % des weltweiten Jahresumsatzes

WICHTIGE EINRICHTUNGEN
bis 7 Mio. €
oder bis 1,4 % des weltweiten Jahresumsatzes

1 **Registrierung**
Eigener Bußgeldtatbestand, bis 500.000 € – unabhängig vom Stand der Technik. Öffentlich bekannte Bußgelder nach BSIG: keine.

2 **Bisherige Praxis**
Erinnerungsmails an die Verbände im Juni und August 2026, Hinweisschreiben an 47 Einrichtungen. Bei weiterhin ausbleibenden Registrierungen zieht das BSI Zwangsgelder und Bußgeldverfahren in Betracht.

Vorgehensweise

Sechs Schritte

1 — SOFORT
Betroffenheit prüfen
Schriftliches Prüfergebnis mit Sektorzuordnung, Schwellenwerten und Konzernbezug.

2 — BIS 30.09.2026
Jetzt registrieren
ELSTER-Organisationszertifikat über „Mein Unternehmenskonto" beantragen, dann im BSI-Portal registrieren.

3 — KURZFRISTIG
Leitung einbinden
Leitungsentscheidung dokumentieren, Schulung der Leitungsebene terminieren.

4 — KURZFRISTIG
Meldeprozess aufsetzen
Eine Faktenbasis für BSI, Datenschutzaufsicht und ENISA, Rufbereitschaft, Vorlagen, Trockenübung.

5 — MITTELFRISTIG
Lieferkette regeln
Vertragsklauseln, Standardantwort auf Fragebögen, Prüfrechte, Lieferantenkategorien.

6 — MITTELFRISTIG
Nachweise aufbauen
Rahmenwerk wählen, § 30-Abgleich dokumentieren, Wirksamkeit in der Managementbewertung feststellen.

Zusammenfassung

Und was kommt jetzt?

1. Die Frage hat sich verschoben: nicht mehr „Sind wir betroffen?", sondern „Können wir belegen, dass wir es geprüft und umgesetzt haben?"
2. Der 30. September ist keine Fristverlängerung, sondern die Ansage des BSI vor Zwangsgeld und Bußgeldverfahren.
3. Die größte Gruppe sind nicht die regulierten Einrichtungen, sondern deren mittelbar betroffene Lieferanten.

Was noch nachkommt

- Cyber Resilience Act: Meldepflicht ab 11.09.2026
- Konkretisierende Rechtsverordnungen zum BSIG
- KRITIS-Dachgesetz: Registrierungsfrist gestrichen, Musterpläne für 2027 angekündigt
- Aktualisierung der Betroffenenzahl durch das Statistische Bundesamt im Herbst 2026 angekündigt

Fragen?

Diskussion!

Vielen Dank für Ihre Aufmerksamkeit!

Konsul-Smidt-Straße 88 • 28217 Bremen
T +49 (0) 421 69 66 32-298
Mail: akademie@dsn-group.de

www.dsn-group.de/dsn-akademie