

CHECKLISTE · NIS2 / BSIG

NIS2- Checkliste

Prüfpunkte für wichtige und besonders wichtige Einrichtungen –
von der Betroffenheit über § 30 BSIG bis zu den Meldefristen.

FÜR 25 BIS 250 MITARBEITENDE

SO NUTZEN SIE DIE LISTE

Ihr Stand auf einen Blick

Das NIS2-Umsetzungsgesetz ist seit dem 6. Dezember 2025 in Kraft (BGBl. 2025 I Nr. 301). Es hat das BSI-Gesetz (BSIG) neu gefasst. Haken Sie ab, was bei Ihnen umgesetzt und dokumentiert ist. Offene Punkte sind Ihre Prioritätenliste.

MELDEFRISTEN NACH § 32 BSIG

24 h

Frühe Erstmeldung nach Kenntnis eines erheblichen Sicherheitsvorfalls

72 h

Meldung mit erster Bewertung, Schweregrad und Auswirkungen

1 Monat

Abschlussmeldung nach der 72-h-Meldung (bei laufendem Vorfall: Fortschrittsmeldung)

Betroffenheit & Registrierung

§§ 28, 33 BSIG

- ☐ Sektor nach Anlage 1 oder 2 BSIG geprüft und dokumentiert
- ☐ Größe ermittelt: Mitarbeitende, Jahresumsatz, Bilanzsumme (KMU-Empfehlung 2003/361/EG, Partner- und verbundene Unternehmen)
- ☐ Einstufung festgehalten: besonders wichtige oder wichtige Einrichtung
- ☐ Registrierung über „Mein Unternehmenskonto“ und BSI-Portal erledigt
- ☐ Änderungen der Registrierungsangaben binnen zwei Wochen melden – Zuständigkeit geregelt

Geschäftsleitung

§ 38 BSIG

- ☐ Risikomanagementmaßnahmen von der Geschäftsleitung umgesetzt und überwacht
- ☐ Regelmäßige Schulung der Geschäftsleitung geplant und nachgewiesen
- ☐ Verantwortlichkeiten für Informationssicherheit benannt

Risikoanalyse & Sicherheitskonzept

§ 30 Abs. 2 Nr. 1 BSIG

- ☐ Inventar der IT-Systeme, Dienste und Daten aktuell
- ☐ Risikoanalyse durchgeführt, Maßnahmen priorisiert
- ☐ Sicherheitsrichtlinien freigegeben und bekannt gemacht

Sicherheitsvorfälle & Meldewege

§ 30 Abs. 2 Nr. 2, § 32 BSIG

- ☐ Prozess zur Erkennung und Bewertung erheblicher Sicherheitsvorfälle
- ☐ Meldekette für 24 h / 72 h / 1 Monat mit Vertretungsregel
- ☐ Vorlagen für Erst-, Folge- und Abschlussmeldung vorbereitet

Betrieb aufrechterhalten

§ 30 Abs. 2 Nr. 3 BSIG

- ☐ Backup-Konzept mit getrennter Kopie, Wiederherstellung regelmäßig getestet
- ☐ Notfall- und Wiederanlaufplan für kritische Systeme
- ☐ Krisenstab und Notfallkommunikation festgelegt

Lieferkette

§ 30 Abs. 2 Nr. 4 BSIG

- ☐ Wesentliche IT-Dienstleister und Lieferanten erfasst
- ☐ Sicherheitsanforderungen vertraglich vereinbart
- ☐ Risiken der Lieferkette regelmäßig bewertet

Beschaffung, Entwicklung, Wartung

§ 30 Abs. 2 Nr. 5 BSIG

- ☐ Sicherheitsanforderungen bei Einkauf und Entwicklung
- ☐ Patch- und Schwachstellenmanagement mit festen Fristen
- ☐ Umgang mit gemeldeten Schwachstellen geregelt

Wirksamkeit prüfen

§ 30 Abs. 2 Nr. 6 BSIG

- ☐ Kennzahlen bzw. Prüfungen zur Wirksamkeit der Maßnahmen
- ☐ Interne Überprüfung in festem Rhythmus

Schulung & Sensibilisierung

§ 30 Abs. 2 Nr. 7 BSIG

- ☐ Grundschulung Informationssicherheit für alle Mitarbeitenden
- ☐ Sensibilisierung zu Phishing und Social Engineering wiederkehrend

Kryptographie

§ 30 Abs. 2 Nr. 8 BSIG

- ☐ Konzept für Verschlüsselung von Daten und Verbindungen
- ☐ Schlüssel- und Zertifikatsverwaltung geregelt

Personal, Zugriff, Assets

§ 30 Abs. 2 Nr. 9 BSIG

- ☐ Ein- und Austrittsprozess mit Rechtevergabe und -entzug
- ☐ Rollen- und Berechtigungskonzept, Admin-Konten getrennt
- ☐ Verwaltung von IKT-Systemen und -Produkten dokumentiert

Authentifizierung & Kommunikation

§ 30 Abs. 2 Nr. 10 BSIG

- ☐ Multi-Faktor-Authentifizierung für relevante Zugänge
- ☐ Gesicherte Sprach-, Video- und Textkommunikation
- ☐ Bei Bedarf gesicherte Notfallkommunikation

Dokumentation

§ 30 Abs. 1 S. 3 BSIG

- ☐ Umsetzung aller Maßnahmen nachvollziehbar dokumentiert
- ☐ Dokumentation aktuell und für Nachweise abrufbar

BUSSGELDRAHMEN NACH § 65 BSIG (AUSZUG)

Verstöße u. a. gegen § 30 (Maßnahmen, Dokumentation) und § 32 (Meldungen): bis 10 Mio. € für besonders wichtige, bis 7 Mio. € für wichtige Einrichtungen. Bei mehr als 500 Mio. € Gesamtumsatz bis 2 % bzw. 1,4 % des weltweiten Gesamtumsatzes, wenn dieser Betrag höher ist.

Hinweis: Diese Checkliste ist eine Arbeitshilfe und keine Rechtsberatung. Sie ersetzt weder die Prüfung des Gesetzestextes noch die Einordnung durch Ihre Rechtsberatung. Quellen: BSIG (gesetze-im-internet.de/bsig_2025), BGBl. 2025 I Nr. 301, BSI. Stand: 23.10.2026.

NÄCHSTER SCHRITT

Sicher zum Wachstum.

Wir unterstützen bei den technischen Maßnahmen mit Managed Security und Cyber Security und dokumentieren den Stand für Ihre Nachweise. BDT ist ISO/IEC 27001 zertifiziert für IT-Infrastrukturberatung und -implementierung.

beratung@blured.de · +49 211 822 00 80
blured.de/nis2/