

Cybersicherheit delegiert — Verantwortung auch?

Die persönlichen Pflichten der Geschäftsleitung nach § 38 BSIG

Juergen L. Sommer · Experte für Digitale Risiken

IHK für Oberfranken Bayreuth · Onlinewebinar · 6. Oktober 2026

Was Sie in den nächsten 45 Minuten erwartet

Warum die Geschäftsleitung

Vier Regulierungen, eine Bewegung — und was das BSIG mit Ihrem Unternehmen zu tun hat

Sind wir regulierungsrelevant

Die zwei Bedingungen, der Zulieferer-Pfad, und warum kein Bescheid kommt

Die drei Pflichten aus § 38

Umsetzen, überwachen, schulen — was Sie abgeben können und was nicht

Was dahinter steht

§ 30 Maßnahmen, § 32 Meldefristen, § 33 Registrierung

Mythen und erste Schritte

Sechs Sätze, die häufig fallen — und was am Montag zu tun ist

Wichtiger Hinweis: Dieses Webinar dient der Orientierung. Es ersetzt keine Rechtsberatung und keine technische IT-Beratung. Es ist keine Schulung nach § 38 Abs. 3 BSIG.

Juergen L. Sommer

Hintergrund

- 30+ Jahre IT-Leadership — T-Systems, IBM, HPE, SUSE, Red Hat
- MBA Corporate Governance, Henley Business School
- Dozent IHK Oberfranken · Hochschule für angewandtes Management

Womit ich arbeite

- Digitale Risiken souverän steuern — Beratung auf Geschäftsleitungsebene
- NIS2/BSIG, EU AI Act, DSGVO, Cyber Resilience Act
- Keine technische IT-Dienstleistung, keine Rechtsberatung

Vier Wirkungsräume, eine Bewegung

Organisation

BSIG

Umsetzung der NIS2-Richtlinie
(EU) 2022/2555.
In Kraft seit 06.12.2025.
Keine Übergangsfrist.

Produkt

CRA · MVO

CRA, VO (EU) 2024/2847:
Meldepflichten nach Art. 14 seit
11.09.2026 an ENISA, übrige
Pflichten ab 11.12.2027.
Maschinenverordnung (EU)
2023/1230 ab 20.01.2027.

Daten

DSGVO

VO (EU) 2016/679.
Gilt seit 2018.
Meldepflicht nach Art. 33 läuft
parallel zum BSIG.

KI

AI Act

VO (EU) 2024/1689.
Art. 4 KI-Kompetenz seit
02.02.2025.
Allgemeiner Geltungsbeginn
02.08.2026.

Zwei Beobachtungen. Dasselbe Unternehmen steht regelmäßig in mehreren Kästen gleichzeitig — als Betreiber im ersten, als Hersteller im zweiten. Und: Alle vier verlangen einen Nachweis statt eines Bemühens. Aber nur einer benennt die Geschäftsleitung persönlich.

Quelle: VO (EU) 2022/2555 · 2024/2847 · 2023/1230 · 2016/679 · 2024/1689

Ein Gesetz über eine Behörde — das Sie verpflichtet

Teile 1 – 2

Allgemeine Vorschriften · Das Bundesamt — Staat

Teil 3

Sicherheit in der Informationstechnik von Einrichtungen — Ihr Unternehmen

Teile 4 – 6

Domain-Registrierungsdaten · Zertifizierung · Verordnungsermächtigungen — überwiegend Staat

Teile 7 – 8

Aufsicht · Bußgeldvorschriften — Ihr Unternehmen

Teil 9

Anwendungsbestimmungen und Übergangsregelungen

66 Paragraphen in neun Teilen. Unmittelbar betreffen Sie davon ein knappes Dutzend — Pflichtenkern sind §§ 30, 32, 33, 35, 36 und 38.
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSIg)

Was Sie abgeben können — und was bei Ihnen bleibt

§ 38 BSIG trägt die amtliche Überschrift „Umsetzungs-, Überwachungs- und Schulungspflicht“. Drei Pflichten. Zwei davon sind nicht delegierbar.

Delegierbar

- Die operative Umsetzung der Maßnahmen nach § 30 BSIG
- An die IT-Leitung, einen externen Dienstleister, einen Informationssicherheitsbeauftragten
- Das ist der Normalfall — und kein Versäumnis

Nicht delegierbar

- Die Überwachung, dass die Maßnahmen umgesetzt sind und wirken (§ 38 Abs. 1)
- Die eigene Schulung (§ 38 Abs. 3)
- Wer delegiert, ohne zu überwachen, hat die Pflicht nicht erfüllt — nur verschoben

Quelle: § 38 BSIG (BGBl. 2025 I Nr. 301, geänd. Art. 4 G v. 11.03.2026)

Wer ist betroffen — der Prüfpfad

Drei Merkmale müssen zusammenkommen: entgeltliches Angebot von Waren oder Dienstleistungen, Zuordnung zu einer Einrichtungsart der Anlage 1 oder 2, Erreichen einer Schwelle. Anlage 1 hat sieben Sektoren, Anlage 2 sieben; zusammen die 14 BSIG-Sektoren.

- 1 **Anlage 1 und ≥ 250 Mitarbeiter oder > 50 Mio. € Umsatz und > 43 Mio. € Bilanzsumme** → besonders wichtige Einrichtung
- 2 **Anlage 1 oder 2 und ≥ 50 Mitarbeiter oder > 10 Mio. € Umsatz und Bilanzsumme** → wichtige Einrichtung
- 3 **Keines von beidem** → nicht direkt reguliert. Der Zulieferer-Pfad bleibt.

Ohne Größenschwelle

Betreiber kritischer Anlagen, qualifizierte Vertrauensdienste, TLD-Registries und DNS-Anbieter (§ 28 Abs. 1 Nr. 1 und 2) sowie Vertrauensdiensteanbieter (§ 28 Abs. 2 Nr. 1). Telekommunikation folgt eigenen Schwellen (§ 28 Abs. 1 Nr. 3, Abs. 2 Nr. 2).

Quelle: § 28 BSIG · §§ 28 Abs. 5 und 6 enthalten Sonderregelungen für Telekommunikation, Energie und Finanzunternehmen

Kritische Anlage — Abgrenzung und Zusatzpflichten

Das Gesetz kennt keine „KRITIS-Firma“. Es kennt die kritische Anlage — wer eine betreibt, ist Betreiber. Die Eigenschaft hängt an der Anlage, die Folgen treffen das Unternehmen.

Vier Schritte — alle müssen zutreffen

- 1 Anlage gehört einem KRITIS-Sektor an
- 2 Sie erbringt eine kritische Dienstleistung für die Allgemeinheit — Eigenversorgung zählt nicht
- 3 Sie fällt unter eine Anlagenkategorie der BSI-Kritisverordnung
- 4 Sie überschreitet den Schwellenwert — Regelwert 500.000 versorgte Personen

Was zu den Pflichten der bwE hinzukommt

§ 31 Abs. 1 Höherer Verhältnismäßigkeitsmaßstab für die Systeme der kritischen Anlage

§ 31 Abs. 2 Systeme zur Angriffserkennung — die einzige technische Maßnahme, die das BSIG namentlich vorschreibt

§ 39 Nachweis durch Audits, Prüfungen oder Zertifizierungen, anschließend alle drei Jahre — turnusmäßig, nicht anlassbezogen

§ 32 Abs. 3 · § 33 Abs. 2 Erweiterte Meldeangaben, Registrierung nach § 8 KRITIS-Dachgesetz

Kein Entweder-oder. § 28 Abs. 1 Nr. 1 macht Betreiber kritischer Anlagen zu besonders wichtigen Einrichtungen. Alle Pflichten der bwE gelten zusätzlich — die kritische Anlage ersetzt nichts, sie liegt auf.

Quelle: §§ 28 Abs. 1 Nr. 1, 31, 32 Abs. 3, 33 Abs. 2, 39 BSIG · BSI-Kritisverordnung · Vorbehalt: § 2 Nr. 22 ist nach § 66 BSIG erst mit Geltung der Rechtsverordnung nach §§ 4 Abs. 3, 5 Abs. 1 KRITIS-Dachgesetz anwendbar; bis dahin gilt die bis 16.03.2026 geltende Fassung.

Was die Kategorie tatsächlich ändert

Besonders wichtige Einrichtungen · § 61

- Das BSI kann Audits, Prüfungen oder Zertifizierungen durch unabhängige Stellen anordnen
- Nachweisvorlage gegenüber weiteren Einrichtungen frühestens drei Jahre nach Inkrafttreten — Krankenhäuser nach § 108 SGB V frühestens fünf Jahre
- Auswahl nach Risikoexposition, Größe, Eintrittswahrscheinlichkeit und Schwere möglicher Vorfälle sowie deren gesellschaftlichen und wirtschaftlichen Auswirkungen (§ 61 Abs. 4)

Wichtige Einrichtungen · § 62

- Das BSI wird nur tätig, wenn Tatsachen die Annahme rechtfertigen, dass Pflichten nicht oder nicht richtig umgesetzt werden
- Dann stehen ihm dieselben Maßnahmen offen
- Ein Vorfall, eine Beschwerde oder eine Meldung reicht als Anlass

Beide Vorschriften nennen § 38 Abs. 3 ausdrücklich als Prüfgegenstand — neben § 30 Abs. 1 Satz 1 und § 32. Die Schulungspflicht ist nicht nur eine Pflicht, sie ist eine prüfbare Pflicht.

Quelle: §§ 61, 62 BSIg · Bußgeldrahmen § 65: bis 10 Mio. € (bwE) / 7 Mio. € (wE) · Zwangsgeld § 63: bis 100.000 €

Betroffen, ohne betroffen zu sein

1

Ihr Kunde ist NIS2-pflichtig. Er muss nach § 30 Abs. 2 Nr. 4 BSIG die Sicherheit der Lieferkette behandeln — einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern.

2

Er reicht das weiter. Fragebögen, Nachweisforderungen, Auditklauseln, Vertragsanpassungen bei der nächsten Verlängerung.

3

Bei Ihnen kommt es an. Nicht als Bescheid der Aufsicht, sondern als Anlage zur Bestellung. Und deutlich früher.

Konsequenz. Wer die Schwellen des § 28 BSIG nicht erreicht, kann faktisch betroffen sein. Nicht über das Gesetz, sondern über den Vertrag. Ein „Wir sind zu klein“ beantwortet die Frage nicht, ob Ihr größter Kunde das genauso sieht.

Quelle: § 30 Abs. 2 Nr. 4 BSIG

Es kommt kein Bescheid

- Die Einstufung ist Selbsteinstufung. Das BSI benachrichtigt betroffene Unternehmen nicht.
- Hilfsmittel: die NIS-2-Betroffenheitsprüfung des BSI unter [betroffenheitspruefung-nis-2.bsi.de](https://bfs.bsi.de/betroffenheitspruefung-nis-2), dazu der Entscheidungsbaum als PDF.
- Was zählt, ist die dokumentierte eigene Bewertung — auch dann, wenn sie „nicht betroffen“ lautet.

Der Vorbehalt, den das BSI selbst formuliert

Die Betroffenheitsprüfung dient lediglich als Orientierungshilfe. Ihr Ergebnis ist rechtlich nicht bindend, weil die Antworten automatisiert erstellt und nicht geprüft werden. Sie ersetzt die Prüfung zur Selbst-Identifizierung nicht und hat für eventuelle Verfahren keine Indizwirkung. Eine verbindliche Mitteilung der individuellen Betroffenheit erfolgt durch das BSI nicht.

Quelle: BSI, NIS-2-Betroffenheitsprüfung · § 28 BSIG

§ 38 Abs. 1 — umsetzen und überwachen

„Geschäftsleitungen ... sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.“

- Die Pflicht trifft die Geschäftsleitung, nicht die Einrichtung. Das ist der Unterschied zu § 30.
- Delegiert werden kann die Umsetzung. Überwachung bleibt beim Organ — sie ist der Teil, der die Delegation überhaupt erst verantwortbar macht.
- „Geschäftsleitung“ ist kein Sammelbegriff: § 2 Nr. 13 BSIG verlangt Berufung zur Führung der Geschäfte und zur Vertretung.
- Nicht „billigen“. Der Begriff stammt aus Art. 20 der NIS2-Richtlinie und steht nicht im BSIG — maßgeblich ist der deutsche Wortlaut.

Quelle: § 38 Abs. 1, § 2 Nr. 13 BSIG

Woran man Überwachung erkennt

Wer

Wer berichtet Ihnen über den Stand der Maßnahmen? Mit Namen, nicht als Abteilung.

Wie oft

In welchem Rhythmus? Ein fester Tagesordnungspunkt trägt weiter als ein Jahresprojekt.

Woran

Woran hätten Sie gemerkt, dass eine Maßnahme nicht mehr wirkt? Wirksamkeit, nicht Aktivität.

Was im Prüffall zählt

§ 30 Abs. 1 Satz 3 BSIG verlangt, die Einhaltung zu dokumentieren — und die fehlende Dokumentation ist ein eigenständiger Bußgeldtatbestand nach § 65 Abs. 2 Nr. 3 BSIG. Sie können also alles richtig gemacht haben und trotzdem sanktioniert werden.

Überwachung zeigt sich nicht daran, was Sie wussten, sondern daran, was nachvollziehbar ist.

Quelle: § 30 Abs. 1 Satz 3 BSIG · § 65 Abs. 2 Nr. 3 BSIG

§ 38 Abs. 3 — die Schulungspflicht

Verlangt wird die regelmäßige Teilnahme an Schulungen, um ausreichende Kenntnisse und Fähigkeiten zu erlangen: zur Erkennung und Bewertung von Risiken, zu Risikomanagementpraktiken und zur Beurteilung der Auswirkungen beider auf die erbrachten Dienste. Drei Kompetenzbereiche, nicht einer.

Geschäftsleitung nach § 2 Nr. 13

- Geschäftsführerinnen und Geschäftsführer einer GmbH
- Vorstandsmitglieder einer AG
- persönlich haftende, vertretungsberechtigte Gesellschafter
- bei der GmbH & Co. KG: die Geschäftsführer der Komplementär-GmbH

Gehört nicht dazu

- Prokuristen — Vertretungsmacht ja, Berufung zur Geschäftsführung nein
- Aufsichtsrat und Beirat
- CIO, CISO, IT-Leitung, sofern nicht zugleich Organ
- Teilnahme kann trotzdem sinnvoll sein — sie ersetzt Ihre aber nicht

Kein Intervall, keine Dauer, kein Format im Gesetz. Vier Anhaltspunkte nennt die BSI-Handreichung: Wechsel in der Geschäftsleitung, signifikante Änderungen der Geschäftsprozesse, der Risikoexposition oder der Maßnahmen.

Quelle: § 38 Abs. 3, § 2 Nr. 13 BSIG · BSI-Handreichung V1.0 vom 17.04.2026, Abschnitte 1.1 und 1.2

§ 38 Abs. 2 — die persönliche Sorgfaltspflicht

„Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts.“

- 1 Innenhaftung.** Gegenüber der eigenen GmbH, AG oder Genossenschaft — nicht gegenüber Dritten und nicht gegenüber der Behörde.
- 2 Kein neuer Haftungstatbestand.** Das BSIG verweist auf das bestehende Gesellschaftsrecht: § 43 GmbHG, § 93 AktG, je nach Rechtsform.
- 3 Auffangregelung.** Nach dem BSIG selbst wird nur gehaftet, wenn das Gesellschaftsrecht keine entsprechende Regelung enthält.

Neu ist nicht die Haftung. Neu ist der Maßstab: § 38 Abs. 1 konkretisiert, woran die Sorgfalt gemessen wird.

Quelle: § 38 Abs. 1 und 2 BSIG · § 43 GmbHG · § 93 AktG

Sanktionen — wen sie treffen

§ 65 richtet sich gegen die Einrichtung

- Maßnahmen nach § 30 Abs. 1 Satz 1 nicht ergriffen
- Dokumentation nach § 30 Abs. 1 Satz 3 fehlt
- Meldung nach § 32 Abs. 1 Satz 1 oder Abschlussmeldung nach § 32 Abs. 2 Satz 2 versäumt
- dafür bis 10 Mio. € (bwE) bzw. 7 Mio. € (wE) — § 65 Abs. 5 Satz 1 Nr. 1
- Registrierung nach § 33 und Verstöße gegen Anordnungen sind ebenfalls bußgeldbewehrt, aber mit eigenen, niedrigeren Rahmen

Die persönliche Ebene

- § 38 Abs. 2 BStG — Innenhaftung gegenüber der eigenen Einrichtung nach Gesellschaftsrecht
- § 61 Abs. 9 BStG — kommt eine Einrichtung Anordnungen des BSI trotz Fristsetzung nicht nach, kann die zuständige Aufsichtsbehörde als letztes Mittel die fachrechtliche Genehmigung aussetzen und unzuverlässigen Geschäftsleitungen die Tätigkeit vorübergehend untersagen
- Zwei Normen, zwei verschiedene Mechanismen — beide unabhängig vom Bußgeld

Ob daneben eine Zurechnung nach dem Ordnungswidrigkeitenrecht in Betracht kommt, ist nicht abschließend geklärt. Umsatzbezogene Bußgeldsätze greifen erst ab 500 Mio. € Gesamtumsatz.

Quelle: § 65 Abs. 5, § 38 Abs. 2, § 61 Abs. 9 BStG · Reichweite des § 61 Abs. 9 gegenüber wichtigen Einrichtungen: nach § 62 zu prüfen

§ 30 — die zehn Maßnahmen

- 1 Risikoanalyse und Sicherheitskonzepte
- 2 Bewältigung von Sicherheitsvorfällen
- 3 Aufrechterhaltung des Betriebs — Backup, Wiederherstellung, Krisenmanagement
- 4 Sicherheit der Lieferkette
- 5 Sicherheit bei Erwerb, Entwicklung und Wartung, inkl. Schwachstellen
- 6 Bewertung der Wirksamkeit der Maßnahmen
- 7 Grundlegende Schulungen und Sensibilisierung
- 8 Kryptographische Verfahren
- 9 Personalsicherheit, Zugriffskontrolle, Verwaltung von IKT-Systemen
- 10 Multi-Faktor-Authentifizierung und gesicherte Kommunikation

→ „Zumindest“ — Absatz 2 Satz 2 formuliert einen Mindestkatalog, keine abschließende Liste.

→ Verhältnismäßigkeit ist eingebaut: Absatz 1 Satz 2 nennt ausdrücklich Risikoexposition, Größe der Einrichtung, Umsetzungskosten sowie Eintrittswahrscheinlichkeit und Schwere.

→ Nummer 7 betrifft die Belegschaft, nicht die Geschäftsleitung. Das ist § 30 — nicht § 38 Abs. 3.

Quelle: § 30 Abs. 1 und 2 BSIG

§ 32 — die Meldekette

24 Stunden

frühe Erstmeldung

Unverzüglich nach Kenntniserlangung. Mit der Angabe, ob der Verdacht auf rechtswidrige Handlungen oder grenzüberschreitende Auswirkungen besteht.

72 Stunden

erste Bewertung

Bestätigung oder Aktualisierung, dazu Schweregrad, Auswirkungen und gegebenenfalls Kompromittierungsindikatoren.

auf Ersuchen

Zwischenmeldung

Relevante Statusaktualisierungen, wenn das BSI sie anfordert.

1 Monat

Abschlussmeldung

Nach der 72-Stunden-Meldung. Dauert der Vorfall an, tritt eine Fortschrittmeldung an ihre Stelle.

Auslöser

Nur der erhebliche Sicherheitsvorfall nach § 2 Nr. 11 — eingetreten oder möglich. Der Beinahevorfall nach § 2 Nr. 1 löst keine Meldepflicht aus.

Der zweite Pfad

Bei Bezug zu personenbezogenen Daten läuft parallel Art. 33 DSGVO, 72 Stunden, an die Datenschutzaufsicht. Zwei Pfade, ein Ereignis.

Quelle: § 32 Abs. 1 und 2, § 2 Nr. 11 und Nr. 1 BSIG · Art. 33 DSGVO

§ 33 — Registrierung

Frist: spätestens drei Monate, nachdem eine Einrichtung erstmals oder erneut als besonders wichtige oder wichtige Einrichtung gilt. Was zu übermitteln ist, liefern drei verschiedene Stellen im Haus.

Geschäftsleitung

Einstufung als besonders wichtige oder wichtige Einrichtung · Sektor nach Anlage 1 oder 2 · Kontaktstelle, die erreichbar ist

Verwaltung

Name mit Rechtsform und Handelsregisternummer · Anschrift und Kontaktdaten · Mitgliedstaaten mit Dienstleistung

IT

Öffentliche IP-Adressbereiche · Zugang über ELSTER-Organisationszertifikat bzw. Mein Unternehmenskonto — Vorlauf mehrere Wochen

Noch zu klären

Die zuständigen Aufsichtsbehörden des Bundes und der Länder — nach § 33 Abs. 1 Nr. 5 benennen Sie sie selbst

§ 33 Abs. 3: Wird die Registrierungspflicht nicht erfüllt, kann das BSI die Registrierung im Einvernehmen mit den zuständigen Aufsichtsbehörden selbst vornehmen.

Quelle: § 33 BSIG · Betreiber kritischer Anlagen: § 8 KRITIS-Dachgesetz

Umsetzung im Mittelstand — fünf Ebenen

1 Technische Stabilität

Backups, Patches, Zugriffsrechte, Netzwerksicherheit. Nicht ob Sie Technik haben — ob sie im Ernstfall funktioniert.

2 Daten & Prozesse

Datenflüsse, kritische Prozesse, Notfallpläne. Könnten Sie innerhalb der Meldefristen melden, was passiert ist?

3 KI & Entscheidungslogik

Welche KI-Werkzeuge nutzen Ihre Mitarbeiter — und wissen Sie davon?

4 Risikomanagement & Verantwortlichkeiten

Wer ist zuständig, mit Namen und dokumentiertem Mandat? Wen nennen Sie, wenn das BSI anruft?

5 Führung & Haftung

Ihre persönlichen Pflichten nach § 38 BStG. Die Ebene, auf der Sie allein stehen.

Ebenen 1 und 2 sind das Feld Ihrer IT und Ihres Dienstleisters. Ab Ebene 3 wird es eine Führungsfrage — genau dort verläuft die Linie aus § 38 Abs. 1.

Sechs Sätze, die häufig fallen

„Wir sind keine kritische Infrastruktur.“

Das BSIG kennt die kritische Anlage (§ 2 Nr. 22) und reguliert die Anlage. Wichtige und besonders wichtige Einrichtung nach § 28 ist eine davon unabhängige Kategorie.

„Wir sind ISO 27001 zertifiziert.“

Deckt einen großen Teil des § 30 ab. Nicht enthalten: §§ 32, 33 und 38. Der ISO-Scope ist frei wählbar, der BSIG-Scope nicht.

„Unser IT-Dienstleister hat das übernommen.“

Der Vertrag wirkt im Innenverhältnis. Adressat der Aufsicht bleibt die Einrichtung, die Überwachungspflicht bleibt beim Organ.

„Wir haben eine Cyberversicherung.“

Versicherung gleicht Schäden aus. Die Pflichten aus §§ 30, 32, 33 und 38 bestehen unabhängig vom Versicherungsvertrag.

„Es gibt sicher eine Übergangsfrist.“

Für die Pflichten aus §§ 30, 32, 33 und 38 gibt es keine Übergangsfrist — sie gelten seit dem 6. Dezember 2025. Die Registrierungsfrist nach § 33 beträgt drei Monate ab Betroffenheit.

„Für die Schulung schicken wir jemanden.“

§ 38 Abs. 3 spricht die Geschäftsleitungen im Plural an — jedes Mitglied persönlich. Prokuristen, Beirat und IT-Leitung gehören nach § 2 Nr. 13 nicht dazu.

Quelle: §§ 2, 28, 30, 32, 33, 38 BSIG · BSI, ISO/IEC 27001 im Kontext NIS2/BSIG

Die ersten fünf Schritte

1

Einstufung durchführen und schriftlich festhalten. Einrichtungsart, Schwelle — und prüfen, ob Kundenverträge Anforderungen durchreichen. Auch ein „nicht betroffen“ gehört in die Akte.

2

Zugang schaffen, bevor die Frist drückt. ELSTER-Organisationszertifikat bzw. Mein Unternehmenskonto prüfen. Voraussetzung für die Registrierung nach § 33, Frist drei Monate.

3

Meldekette festlegen, bevor etwas passiert. Wer stellt Erheblichkeit fest, wer setzt die 24-Stunden-Meldung ab, wer die nach Art. 33 DSGVO — mit Namen, Vertretung, Erreichbarkeit.

4

Einmal berichten lassen. Stand der zehn Maßnahmen nach § 30 Abs. 2 samt Dokumentation nach Abs. 1 Satz 3. Als Tagesordnungspunkt, nicht als Projekt.

5

Die eigene Schulung terminieren und das Intervall beschließen. § 38 Abs. 3. Das Intervall legt die Geschäftsleitung selbst fest — schriftlich, dann ist es begründet.

Vielen Dank.

**Dieses Webinar dient der Orientierung. Es ersetzt keine Rechtsberatung und keine technische IT-Beratung.
Es ist keine Schulung nach § 38 Abs. 3 BSIG.**

Für die Schulungspflicht

NIS2-Geschäftsleitungsschulung nach § 38 BSIG
IHK für Oberfranken Bayreuth · online

27.10.2026, 09:00–13:00 Uhr
Kursnummer ONLINE-VSNIS0126
Anmeldung über ihk-lernen.de

Weitere Termine 2027: 16.02. · 27.04. · 22.06. · 12.10.

Kontakt

Juergen L. Sommer
Digitale Risiken souverän steuern

juergensommer.de
jls@juergensommer.de
+49 173 4092352

Ihre Fragen

Was ich nicht beantworten kann: die Einstufung Ihres konkreten Falls und Rechtsfragen im Einzelfall.