Vertraglicher Anhang Lieferkettensicherheit nach BSIG / NIS2 – Strukturmuster

Muster-Template (Teaser-Version) zur Absicherung der Lieferkette gemäß § 30 Abs. 2 Nr. 4 BSIG

Teil A – Problemaufriss und Anwendungskontext

1. Warum dieser Sicherheitsanhang?

Mit dem Inkrafttreten des umgesetzten NIS2-Regimes verpflichtet das BSI-Gesetz (BSIG) besonders wichtige und wichtige Einrichtungen ausdrücklich dazu, die Sicherheit ihrer Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern und Diensteanbietern durch geeignete, verhältnismäßige und wirksame Maßnahmen sicherzustellen (§ 30 Abs. 2 Nr. 4 BSIG). Verstöße können Bußgelder von bis zu 2 % des weltweiten Konzernumsatzes (§ 65 BSIG) sowie persönliche Haftung der Geschäftsleitung (§ 38 BSIG) auslösen.

2. Bidirektionaler Anwendungsbereich

Dieser Sicherheitsanhang adressiert **beide Seiten** der NIS2-Lieferkette:

- **Top-down-Perspektive (NIS2-verpflichtetes Unternehmen → Lieferant):** Direkt betroffene Einrichtungen benötigen ein belastbares, BSIG-konformes Vertragswerk, um ihre eigenen gesetzlichen Pflichten in die Lieferkette zu verlängern.
- **Bottom-up-Perspektive (Lieferant → mehrere NIS2-Kunden):** Unternehmen, die Teil kritischer Lieferketten sind, ohne selbst direkt betroffen zu sein, sehen sich oft mit dutzenden uneinheitlichen Sicherheitsanhängen ihrer Kunden konfrontiert. Ein einheitlich strukturiertes Vertragswerk gegenüber verschiedenen Kunden reduziert Komplexität, schafft Verhandlungssicherheit und ermöglicht eine konsistente Compliance-Steuerung.

Teil B – Grundlegendes Vertragstemplate

Präambel

Der Auftraggeber [x] erbringt Leistungen als [besonders wichtige Einrichtung / wichtige Einrichtung / Teil einer kritischen Lieferkette] im Sinne des BSIG. Zur Erfüllung der Pflichten aus § 30 BSIG sowie zur Sicherstellung eines angemessenen Sicherheitsniveaus in der Lieferkette vereinbaren die Parteien folgenden Sicherheitsanhang, der integraler Bestandteil des Hauptvertrages [x] ist.

§ 1 Geltungsbereich und Begriffsbestimmungen

- Anwendungsbereich unter dem Hauptvertrag
- Definitionen: „Sicherheitsvorfall", „erheblicher Sicherheitsvorfall", „Schwachstelle", „kritische Komponente", „Schutzbedarf", „Stand der Technik", „Kenntnis" etc. (in Anlehnung an § 2 BSIG und einschlägige BSI-Definitionen).

§ 2 Risikoklassen und Verhältnismäßigkeit

- Risikoklassen niedrig / mittel / hoch / sehr hoch
- Bewertungskriterien: Schutzbedarf, Kritikalität, Datenumfang, Substituierbarkeit
- Skalierung der Pflichten je Risikoklasse
- Regelmäßige Überprüfung
- Verhältnismäßigkeitsmaßstab (Risikoexposition, Größe, Kosten, Eintrittswahrscheinlichkeit, Schwere)

§ 3 Allgemeine Sicherheitspflichten und Informationssicherheits-Managementsystem (ISMS)

3.1 Stand der Technik

- Geeignete, verhältnismäßige, wirksame TOMs nach Stand der Technik
- Anlehnung an BSI IT-Grundschutz

3.2 Informationssicherheits-Managementsystem (ISMS)

- Dokumentiertes ISMS nach anerkanntem Standard (ISO/IEC 27001:2022, BSI-Standard 200-1/200-2, TISAX, BSI C5)
- Nachweisführung
- Optionsvarianten: Zertifizierungspflicht / gleichwertige Nachweise / risikoklassenabhängig

3.3 Security by Design und Security by Default

- Sicherheitsintegration in Entwicklung und Bereitstellung
- Sichere Standardkonfiguration

3.4 Kryptografie, Zugriffskontrolle und Multi-Faktor-Authentifizierung

- Einsatz kryptografischer Verfahren nach Stand der Technik

- Grundsätze der Zugriffskontrolle (Need-to-know, Least-Privilege)
- Multi-Faktor-Authentifizierung für privilegierte Zugriffe und Fernzugänge
- Konkretisierung in Anlage A (TOMs)

3.5 Zertifizierte IKT-Produkte und branchenspezifische Sicherheitsstandards (B3S)

- Verwendung zertifizierter IKT-Produkte, -Dienste und -Prozesse, soweit durch Rechtsverordnung nach § 30 Abs. 6 BSIG gefordert
- Öffnungsklausel für branchenspezifische Sicherheitsstandards (B3S) nach § 30 Abs. 8, 9 BSIG
- Anerkennung bereits vorhandener Zertifizierungen des Auftragnehmers als Nachweis

3.6 Kontinuierliche Verbesserung

- Jährliche und anlassbezogene Wirksamkeitsprüfung
- Anpassung an Bedrohungslage und Stand der Technik

§ 4 Technische und Organisatorische Maßnahmen (TOMs)

- Detaillierter TOM-Katalog gemäß Anlage A, risikoklassenbasiert skaliert (in Anlehnung an § 30 Abs. 2 BSIG und BSI-Grundschutz).
- Mindestinhalte: Zugriffskontrolle, MFA, Verschlüsselung, Netzwerksicherheit, Logging und Monitoring, Backup und Wiederherstellung, physische Sicherheit, Personalsicherheit, sichere Entwicklung, Business Continuity Management

§ 5 Schwachstellen- und Patchmanagement

- Prozess zur Identifikation, Bewertung (CVSS) und Behebung von Schwachstellen
- Patchfristen nach Kritikalität
- Coordinated Vulnerability Disclosure (CVD)
- Optional: Software Bill of Materials (SBOM) bei IT-Produkten in höherer Risikoklasse

§ 6 Business Continuity, Resilienz und Diversifikation

6.1 Business Continuity Management (BCM)

- Notfallkonzept und Wiederanlaufplanung
- RTO- und RPO-Vorgaben nach Risikoklasse
- Jährliche Notfallübungen

6.2 Erhöhte Anforderungen bei KRITIS-relevanten Leistungen (§ 31 BSIG)

- Systeme zur Angriffserkennung (SzA) beim Auftragnehmer, soweit kritische Leistungen für KRITIS-Anlagen erbracht werden
- Verschärfte Anforderungen an Verfügbarkeit und Wiederherstellung
- Erweiterte Nachweispflichten

6.3 Diversifikation und Alternativlieferanten

- Bei Risikoklasse „hoch" oder „sehr hoch": Bereithaltung alternativer Bezugsquellen bzw. Fallback-Mechanismen
- Pflicht zur Information über wesentliche Konzentrationsrisiken in der eigenen Lieferkette

§ 7 Meldepflichten bei Sicherheitsvorfällen und Schwachstellen

7.1 Grundsatz

- Meldung von Sicherheitsvorfällen und Schwachstellen mit Auswirkung auf den Auftraggeber
- Unabhängig von eigener BSIG-Meldepflicht des Auftragnehmers

7.2 Stufe 1 – Sofortinformation bei begründetem Verdacht

- Unverzügliche Information bei Verdachtsbegründung
- Zweck: Schadensabwehr, nicht formelle Meldung
- Auslösetatbestände (Kompromittierungsindikatoren, unbefugte Zugriffe, wesentliche Leistungsausfälle)

7.3 Stufe 2 – Erstmeldung

- Unverzüglich, spätestens 24 Stunden nach Kenntnis der zuständigen Sicherheitsstelle
- Mindestinhalte: Beschreibung, betroffene Systeme/Daten/Leistungen, ergriffene Maßnahmen, Ansprechperson
- Angelehnt an § 32 Abs. 1 BSIG

7.4 Stufe 3 – Folgemeldungen und Abschlussbericht

- Aktualisierung nach 72 Stunden
- Abschlussbericht nach einem Monat
- Zwischenberichte bei andauerndem Vorfall

7.5 Schwachstellenmeldungen

- Sicherheitskritische Schwachstellen (CVSS ≥ [7,0]): Meldung nach vereinbartem Prozess, spätestens innerhalb von [7] Tagen

7.6 Mitwirkung bei behördlichen Meldungen des Auftraggebers

- Unterstützung bei Meldungen nach § 32 BSIG
- Unterstützung bei Auskunftsersuchen nach § 61 BSIG

7.7 Unterrichtung von Diensteempfängern (§ 35 BSIG)

- Mitwirkung bei Warn- und Unterrichtungspflichten des Auftraggebers gegenüber dessen Diensteempfängern
- Bereitstellung erforderlicher Informationen und Textbausteine

7.8 Sektorspezifische Verschärfungen

- Anpassungsmöglichkeit bei kürzeren regulatorischen Meldefristen des Auftraggebers (z. B. DORA)
- Verhältnismäßigkeitsvorbehalt

§ 8 Einbindung von Unterauftragnehmern (Flow-down)

8.1 Grundsatz der Weitergabe von Sicherheitspflichten

- Volle Verantwortung des Auftragnehmers
- Schriftliche Vereinbarung gleichwertiger Sicherheitsanforderungen mit kritischen Unterauftragnehmern

8.2 Transparenz über die Lieferkette

- Verzeichnis wesentlicher Unterauftragnehmer (Anlage D)
- Pflicht zur proaktiven Information über Änderungen

8.3 Zustimmungs- oder Widerspruchsrecht bei kritischen Unterauftragnehmern

- Optionsvarianten: Zustimmungserfordernis / Widerspruchsrecht mit Vorlauffrist / bloße Informationspflicht

8.4 Untersagung unzuverlässiger Unterauftragnehmer

- Untersagungsrecht bei Sicherheitsbedenken, behördlicher Einstufung oder Vorgaben nach § 41 BSIG

8.5 Verantwortung und Haftung

- Zurechnung von Handlungen der Unterauftragnehmer
- Fortgeltung der Meldepflichten (§ 7)

§ 9 Nachweis- Audit und Kontrollrechte

9.1 Nachweise

- Zertifikate, Auditberichte (ISAE 3402, SOC 2 Typ II), Selbstauskünfte, Penetrationstestberichte

9.2 Audit-Recht

- Dokumentenaudit mit angemessener Vorlauffrist
- Vor-Ort-Audit risikoklassenabhängig oder anlassbezogen
- Pooled-Audit-Option (gemeinsame Audits mit anderen Kunden zur Entlastung des Auftragnehmers)

9.3 Behördliche Prüfungen

- Duldungs- und Mitwirkungspflicht bei BSI-Prüfungen nach § 61 BSIG

9.4 Schutz des Auftragnehmers

- Schonende Durchführung
- Vertraulichkeit der Auditergebnisse
- Schutz von Geschäfts- und Betriebsgeheimnissen sowie Rechten Dritter
- Kostentragung

§ 10 Kritische Komponenten und Untersagungsfall (§ 41 BSIG)

- Kooperationspflicht bei behördlicher Untersagung nach § 41 BSIG
- Austauschpflicht für untersagte Komponenten
- Nachverfolgbarkeit der Lieferkette bei kritischen Komponenten in höherer Risikoklasse
- Kostentragungsregelung

§ 11 Schulung und Awareness

11.1 Schulung und Awareness

- Regelmäßige Schulungen aller Mitarbeitenden mit Bezug zur Leistungserbringung
- Spezifische Awareness-Programme für sicherheitskritische Funktionen
- Nachweispflicht auf Anforderung

11.2 Sicherheitsüberprüfung des Personals (optional)

- Bei Personal mit Zugriff auf Daten oder Systeme mit Schutzbedarf „hoch" oder „sehr hoch"
- Angemessene Zuverlässigkeitsprüfung im Rahmen des rechtlich Zulässigen
- Regelung von Personalwechseln bei sicherheitskritischen Rollen

§ 12 Dokumentations- und Berichtspflichten

- Vorhaltung aktueller Sicherheitsdokumentation
- Jährlicher Sicherheitsbericht (Auditergebnisse, Vorfallstatistik, Schwachstellenstatus, geplante Maßnahmen)
- Aufbewahrungsfristen

§ 13 Beendigung und Exit-Management

- Geordnete Übergabe bei Vertragsende
- Datenrückgabe und nachweisliche Datenlöschung (BSI-konform)
- Asset-Rückgewähr
- Übergangsunterstützung an Nachfolger
- Fortgeltung von Vertraulichkeits- und Sicherheitspflichten

§ 14 Haftung, Vertragsstrafen und Versicherung

- Haftung für Schäden aus Verletzung der Sicherheitspflichten
- Differenzierte Haftungsgrenzen
- Vertragsstrafen für besonders schwerwiegende Pflichtverletzungen (z. B. Verletzung Meldepflichten)
- Mindestversicherungssumme Cyber-Haftpflicht

- Interessenausgleich: Begrenzung außerhalb Vorsatz/grober Fahrlässigkeit, Pauschalierung und Deckelung

§ 15 Verhältnismäßigkeit, Änderungsmechanismus und Schutz vor unverhältnismäßiger Pflichtenverschärfung

- Anpassungspflicht bei wesentlichen Änderungen der Rechtslage, des Stands der Technik oder der Bedrohungslage
- Geordnetes Change-Verfahren mit angemessenen Umsetzungsfristen
- Kostentragung bei wesentlichen Mehraufwänden nach Verhältnismäßigkeitsmaßstab
- Ausdrücklicher Schutzmechanismus für den Auftragnehmer gegen einseitige Pflichtenausweitung
- Spiegel des § 30 Abs. 1 S. 2 BSIG

§ 16 Schlussbestimmungen

- Salvatorische Klausel
- Schriftformerfordernis für Änderungen
- Vorrang dieses Anhangs vor entgegenstehenden Regelungen des Hauptvertrages in Sicherheitsfragen
- Gerichtsstand und anwendbares Recht

Teil C – Anlagen (Übersicht)

Anlage	Inhalt
Anlage A	Technische und Organisatorische Maßnahmen (TOMs), risikoklassenbasiert
Anlage B	Meldeformular Sicherheitsvorfälle + Kontaktdatenmatrix (Incident Response)
Anlage C	Risikoklassen-Matrix (Schutzbedarf × Kritikalität → Pflichtenintensität)
Anlage D	Verzeichnis wesentlicher Unterauftragnehmer (Flow-down-Transparenz)
Anlage E *(optional)*	Modul Cloud-Dienste (in Anlehnung an BSI C5)
Anlage F *(optional)*	Modul Outsourcing/Managed Services