NIS2 LIEFERKETTENSICHERHEIT

NIS2 Lieferketten-Vertragsklauseln

Musterklauseln für § 30 Abs. 2 Nr. 4 BSIG

Muster zur freien Verwendung — keine Rechtsberatung

VERSION
1.0

STAND
4. Juni 2026

LIZENZ
Creative Commons CC-BY-4.0

Präambel und rechtlicher Hinweis

Diese Vertragsklausel-Vorlage dient der Umsetzung der Lieferkettensicherheitsanforderungen nach § 30 Abs. 2 Nr. 4 BSIG (NIS2UmsuCG, in Kraft seit 06.12.2025). Sie enthält sieben Musterklauseln, die als Ergänzung zu bestehenden Lieferanten- oder Dienstleistungsverträgen genutzt werden können. Die Klauseln sind auf Tier-A-Lieferanten (kritisch) ausgerichtet und können für Tier-B-Lieferanten (wichtig) auf die Klauseln 1-4 reduziert werden.

RECHTLICHER HINWEIS

Diese Vorlage ist kein Rechtsrat und ersetzt nicht die Prüfung durch einen qualifizierten Rechtsanwalt. Vor Einsatz in konkreten Vertragsverhandlungen wird eine anwaltliche Prüfung dringend empfohlen. Die Nutzung erfolgt auf eigene Verantwortung. Kopexa GmbH übernimmt keine Haftung für die rechtliche Eignung dieser Muster für konkrete Vertragssituationen.

GESETZLICHE GRUNDLAGE

§ 30 Abs. 2 Nr. 4 BSIG i.V.m. Art. 21 Abs. 2 lit. d NIS2-Richtlinie (EU) 2022/2555. Gilt für besonders wichtige Einrichtungen (§ 28 Abs. 1 BSIG) und wichtige Einrichtungen (§ 28 Abs. 2 BSIG) gemäß BSIG-NIS2UmsuCG, in Kraft seit 06.12.2025.

KLAUSELN 1-3 · SECURITY · INCIDENT · AUDIT

Klauseln 1-3: Sicherheit, Meldung, Audit

Diese drei Klauseln bilden das Fundament der Lieferkettensicherheit: das geforderte Sicherheitsniveau, die Vorfallmeldepflicht des Lieferanten und dein Recht auf Prüfung.

Klausel 1 — Sicherheitsniveau

[NAME DES LIEFERANTEN] (nachfolgend Auftragnehmer) verpflichtet sich, für alle Systeme, Prozesse und Daten, die im Zusammenhang mit der Leistungserbringung für [NAME DES AUFTRAGGEBERS] (nachfolgend Auftraggeber) stehen, ein Informationssicherheitsniveau einzuhalten, das dem aktuellen Stand der Technik entspricht. Der Auftragnehmer hat ein Informationssicherheits-Managementsystem (ISMS) gemäß ISO/IEC 27001 oder einen gleichwertigen Rahmen (BSI IT-Grundschutz, BSI C5) eingerichtet und aufrechtzuerhalten und dem Auftraggeber auf Anfrage einen gültigen Zertifizierungsnachweis vorzulegen. Änderungen, die das Sicherheitsniveau wesentlich beeinflussen könnten, sind dem Auftraggeber unverzüglich, spätestens innerhalb von [ANZAHL] Werktagen, mitzuteilen.

Klausel 2 — Vorfallmeldepflicht

Der Auftragnehmer verpflichtet sich, dem Auftraggeber jeden Sicherheitsvorfall, der die im Rahmen dieses Vertrags bereitgestellten Systeme, Dienste oder Daten des Auftraggebers betreffen könnte, unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach eigener Kenntnisnahme, schriftlich oder per E-Mail an [KONTAKT-E-MAIL] zu melden. Die Meldung muss mindestens folgende Angaben enthalten: Zeitpunkt und Art des Vorfalls, betroffene Systeme und Daten, erste Bewertung des Schweregrads sowie die bereits eingeleiteten Sofortmaßnahmen. Diese Pflicht gilt unabhängig davon, ob der Vorfall beim Auftragnehmer oder einem seiner Subunternehmer eingetreten ist. Der Auftragnehmer kooperiert vollumfänglich bei der Aufklärung des Vorfalls und der Umsetzung von Abhilfemaßnahmen.

Klausel 3 — Audit-Rechte

Der Auftraggeber oder ein von ihm beauftragter Dritter ist berechtigt, das Informationssicherheitsniveau des Auftragnehmers mindestens einmal jährlich zu prüfen. Die Prüfung kann als Fragebogen-Assessement, Dokumentenprüfung oder Vor-Ort-Audit erfolgen. Der Auftragnehmer ist verpflichtet, vollständige und wahrheitsgemäße Auskunft zu erteilen sowie relevante Dokumentation (Richtlinien, Nachweise, Protokolle) zur Verfügung zu stellen. Die Kosten der jährlichen Regelprüfung trägt der Auftraggeber. Bei begründetem Verdacht auf einen Sicherheitsvorfall oder eine wesentliche Sicherheitsabweichung ist der Auftraggeber zur unangekündigten Prüfung berechtigt; die Kosten trägt in diesem Fall der Auftragnehmer, sofern der Verdacht bestätigt wird.

KLAUSELN 4-5 · SUBCONTRACTORS · DATA

Klauseln 4-5: Subunternehmer, Datenlokalisierung

Klausel 4 verhindert unkontrollierte Subunternehmer-Ketten. Klausel 5 sichert die Datenlokalisierung ab und schützt vor unerwünschten Drittland-Transfers.

Klausel 4 — Subunternehmer

Der Auftragnehmer darf Leistungen, die im Rahmen dieses Vertrags erbracht werden und Zugang zu Systemen oder Daten des Auftraggebers umfassen, nur mit vorheriger schriftlicher Zustimmung des Auftraggebers an Subunternehmer weitergeben. Der Auftragnehmer ist verpflichtet sicherzustellen, dass alle Subunternehmer, die im Auftrag des Auftragnehmers auf Systeme oder Daten des Auftraggebers zugreifen, denselben Sicherheitsanforderungen unterliegen wie der Auftragnehmer selbst. Auf Anfrage stellt der Auftragnehmer dem Auftraggeber eine aktuelle Liste aller eingesetzten Subunternehmer zur Verfügung. Änderungen in der Subunternehmerkette sind dem Auftraggeber mindestens [ANZAHL] Werktage im Voraus mitzuteilen.

Klausel 5 — Datenlokalisierung

Alle Daten des Auftraggebers — einschließlich personenbezogener Daten, Geschäftsgeheimnisse und sicherheitsrelevanter Informationen — dürfen ausschließlich in den folgenden Rechtsräumen verarbeitet und gespeichert werden: [LÄNDER / RECHTSRÄUME]. Eine Verlagerung der Datenverarbeitung oder -speicherung in andere Rechtsräume ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftragnehmer gewährleistet, dass alle eingesetzten Subunternehmer und Cloud-Dienste ebenfalls diese Anforderung einhalten. Bei Nichteinhaltung ist der Auftraggeber zur außerordentlichen Kündigung berechtigt.

KLAUSELN 6-7 · BC/RPO · PENALTIES

Klauseln 6-7: Business Continuity, Vertragsstrafen

Klausel 6 sichert die Betriebskontinuität mit konkreten RPO/RTO-Werten. Klausel 7 schafft mit Vertragsstrafen einen finanziellen Anreiz zur Einhaltung.

Klausel 6 — Business Continuity und RPO/RTO

Der Auftragnehmer hält dokumentierte Business-Continuity- und Disaster-Recovery-Pläne vor und testet diese mindestens einmal jährlich. Für kritische Systeme und Daten garantiert der Auftragnehmer einen Recovery Point Objective (RPO) von maximal [RPO] Stunden und einen Recovery Time Objective (RTO) von maximal [RTO] Stunden. Der Auftragnehmer informiert den Auftraggeber unverzüglich über jeden Ausfall, der die vereinbarten RPO/RTO-Zeiten zu überschreiten droht, und legt auf Anfrage aktuelle Testergebnisse und Prüfberichte vor. Die Pläne sind dem Auftraggeber auf Anfrage in zusammengefasster Form zur Einsicht vorzulegen.

Klausel 7 — Vertragsstrafen

Bei Verletzung der in Klausel 2 vereinbarten Vorfallmeldepflicht ist eine Vertragsstrafe in Höhe von [BETRAG] EUR fällig. Bei Verletzung der in Klausel 3 vereinbarten Audit-Verpflichtungen (insbesondere Verweigerung oder wesentliche Behinderung einer Prüfung) ist eine Vertragsstrafe in Höhe von [BETRAG] EUR fällig. Vertragsstrafen sind auf weitergehende Schadensersatzansprüche des Auftraggebers anrechenbar. Das Recht zur außerordentlichen Kündigung des Vertrags bei schwerwiegenden oder wiederholten Verstößen gegen Sicherheitspflichten bleibt unberührt. Die Geltendmachung einer Vertragsstrafe schließt die Kündigung nicht aus.