NIS2 SUPPLY-CHAIN SECURITY

NIS2 Supply-Chain Contract Clauses

Model clauses for § 30(2) No. 4 BSIG

Template for free use — not legal advice

VERSION
1.0

DATE
April 29, 2026

LICENCE
Creative Commons CC-BY-4.0

Preamble and Legal Notice

This contract clause template is designed to support implementation of the supply-chain security requirements under § 30(2) No. 4 BSIG (NIS2UmsuCG, in force since 06 December 2025). It contains seven model clauses that can be used as an addendum to existing supplier or service agreements. The clauses are tailored to Tier-A (critical) suppliers and may be reduced to clauses 1-4 for Tier-B (important) suppliers.

LEGAL NOTICE

This template does not constitute legal advice and does not replace review by qualified legal counsel. Legal review before use in actual contract negotiations is strongly recommended. Use is at your own risk. Kopexa GmbH accepts no liability for the legal suitability of these model clauses for any particular contractual situation.

REGULATORY BASIS

§ 30(2) No. 4 BSIG in conjunction with Art. 21(2)(d) NIS2 Directive (EU) 2022/2555. Applies to essential entities (§ 28(1) BSIG) and important entities (§ 28(2) BSIG) under BSIG-NIS2UmsuCG, in force since 06 December 2025.

KLAUSELN 1-3 · SECURITY · INCIDENT · AUDIT

Clauses 1-3: Security, Reporting, Audit

These three clauses form the foundation of supply-chain security: the required security level, the supplier's incident reporting obligation, and your right to audit.

Clause 1 — Security Level

[SUPPLIER NAME] (hereinafter Contractor) undertakes to maintain an information security level consistent with the current state of the art for all systems, processes, and data related to the provision of services to [CLIENT NAME] (hereinafter Client). The Contractor shall establish and maintain an information security management system (ISMS) in accordance with ISO/IEC 27001 or an equivalent framework (BSI IT-Grundschutz, BSI C5) and shall provide the Client with a valid certification certificate on request. Any changes that could materially affect the security level shall be communicated to the Client immediately, and no later than within [NUMBER] working days.

Clause 2 — Incident Reporting Obligation

The Contractor undertakes to notify the Client of any security incident that could affect the Client's systems, services, or data provided under this agreement, immediately and no later than 24 hours after the Contractor becomes aware of the incident, in writing or by e-mail to [CONTACT EMAIL]. The notification must include at a minimum: the time and nature of the incident, the affected systems and data, an initial assessment of severity, and the immediate measures already taken. This obligation applies regardless of whether the incident occurred at the Contractor or one of its subcontractors. The Contractor shall cooperate fully in investigating the incident and implementing remediation measures.

Clause 3 — Audit Rights

The Client, or a third party appointed by the Client, is entitled to assess the Contractor's information security posture at least once per year. The assessment may take the form of a questionnaire assessment, document review, or on-site audit. The Contractor is obliged to provide complete and accurate information and to make available relevant documentation (policies, evidence, logs). The costs of the annual routine assessment are borne by the Client. In the event of reasonable suspicion of a security incident or material security deviation, the Client is entitled to carry out an unannounced assessment; in this case, the costs shall be borne by the Contractor if the suspicion is confirmed.

KLAUSELN 4-5 · SUBCONTRACTORS · DATA

Clauses 4-5: Subcontractors, Data Localisation

Clause 4 prevents uncontrolled subcontractor chains. Clause 5 secures data localisation and protects against unwanted third-country transfers.

Clause 4 — Subcontractors

The Contractor may only pass on services under this agreement that involve access to the Client's systems or data to subcontractors with the Client's prior written consent. The Contractor shall ensure that all subcontractors acting on the Contractor's behalf who access the Client's systems or data are subject to the same security requirements as the Contractor. On request, the Contractor shall provide the Client with an up-to-date list of all subcontractors engaged. Changes to the subcontractor chain shall be notified to the Client at least [NUMBER] working days in advance.

Clause 5 — Data Localisation

All of the Client's data — including personal data, trade secrets, and security-sensitive information — may only be processed and stored in the following jurisdictions: [COUNTRIES / JURISDICTIONS]. Any transfer of data processing or storage to other jurisdictions requires the Client's prior written consent. The Contractor shall ensure that all subcontractors and cloud services used also comply with this requirement. Non-compliance entitles the Client to terminate the agreement with immediate effect.

KLAUSELN 6-7 · BC/RPO · PENALTIES

Clauses 6-7: Business Continuity, Penalties

Clause 6 secures operational continuity with concrete RPO/RTO values. Clause 7 creates a financial incentive for compliance through contractual penalties.

Clause 6 — Business Continuity and RPO/RTO

The Contractor shall maintain documented business continuity and disaster recovery plans and test them at least once per year. For critical systems and data, the Contractor guarantees a Recovery Point Objective (RPO) of no more than [RPO] hours and a Recovery Time Objective (RTO) of no more than [RTO] hours. The Contractor shall notify the Client immediately of any outage that risks exceeding the agreed RPO/RTO times and shall provide current test results and audit reports on request. The plans shall be made available to the Client in summary form on request.

Clause 7 — Contractual Penalties

A breach of the incident reporting obligation agreed in Clause 2 shall give rise to a contractual penalty of [AMOUNT] EUR. A breach of the audit obligations agreed in Clause 3 (in particular refusal or material obstruction of an assessment) shall give rise to a contractual penalty of [AMOUNT] EUR. Contractual penalties are credited against any further damages claims by the Client. The right to terminate the agreement for cause in the event of serious or repeated breaches of security obligations remains unaffected. Enforcement of a contractual penalty does not preclude termination.