NIS 2 Lieferanten-Fragebogen

Offener, EU-verankerter Fragebogen für die Lieferantenbewertung unter NIS 2

Version 3.1.0 - Stand 2026-05-15 - 59 Felder in 6 Sektionen

Jedes Feld ist an eine EU-rechtliche Primärquelle verankert: NIS 2 Art. 21(2), CIR 2024/2690, ENISA Technical Implementation Guidance, DSGVO Art. 28 oder den Cyber Resilience Act. Sektorspezifische Erweiterungen (TISAX, VDA ISA, BSI C5, KRITIS) ergänzen die Basis, ersetzen sie nicht.

Quelle: github.com/NISD2/nis2-supply-chain-questionnaire-schema (MIT + CC BY 4.0)

1. Lieferantenprofil (18 Felder)

Firmierung (Rechtsname)

[string] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2

Erforderlich nach CIR 2024/2690 §5.2(a) — Lieferantenregister-Eintrag.

Geschäftsanschrift

[string] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2

Erforderlich nach CIR 2024/2690 §5.2(a) — Lieferantenregister-Eintrag.

Land

[country] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2

ISO 3166-1 Alpha-2-Code, z. B. DE, FR, IT.

Primäre Domain

[url] Optional - Rechtsgrundlage: ENISA TIG §5.2(b)

Die primäre öffentliche Domain des Lieferanten.

Slogan (eine Zeile, kundenseitig sichtbar)

[string] Optional - Rechtsgrundlage: ENISA TIG §5.2(b)

Kurze Beschreibung für Kunden.

Öffentliche Beschreibung (länger)

[text] Optional - Rechtsgrundlage: ENISA TIG §5.2(b)

Längere Beschreibung des Lieferanten.

Beschreibung der erbrachten Leistungen

[text] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2(b) + §5.1.4 TIPS

Erforderlich nach ENISA TIG §5.2(b) + §5.1.4 TIPS — klare und vollständige Beschreibung der angebotenen IKT-Produkte und -Dienstleistungen. Ein Absatz.

Länder / Regionen, in denen Kundendaten verarbeitet werden

[string] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.1.4 TIPS

Erforderlich nach ENISA TIG §5.1.4 TIPS — alle Länder / Regionen auflisten, in denen Kundendaten erstellt, verarbeitet oder gespeichert werden. Komma-getrennt.

Name des Sicherheitskontakts

[string] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(d)

Erforderlich nach CIR 2024/2690 §5.1.4(d) — Meldekette für Sicherheitsvorfälle.

E-Mail für Vorfälle

[email] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(d)

Standard-E-Mail für Vorfallsmeldungen durch Kunden.

Telefonnummer für Vorfälle (24/7)

[phone] Optional - Rechtsgrundlage: CIR 2024/2690 §5.1.4(d)

24/7-Telefon für kritische Vorfallsmeldungen.

Meldefrist für Vorfälle (Stunden)

[integer] Optional - Rechtsgrundlage: NIS2 Art. 23

Maximale Zeit von Vorfallserkennung bis Kundenbenachrichtigung.

BSI-Registrierungs-ID (nur falls Ihr Unternehmen selbst NIS2-reguliert ist)

[string] Optional - Rechtsgrundlage: ENISA TIG §5.1.2

Optional. ENISA TIG §5.1.2 — falls Ihr Unternehmen selbst NIS2-reguliert mit BSI-Registrierung ist, können Ihre Kunden diese Tatsache zur Erfüllung ihrer §5.1.2 Lieferantenauswahlkriterien nutzen.

Wir bieten SaaS / gehostete Dienste

[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2(b)

Bestimmt, welche technischen Fragen als Nächstes erscheinen. Mehrfachauswahl möglich.

Wir liefern On-Prem-Software

[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2(b)

Software, die Ihre Kunden auf eigener Hardware betreiben.

Wir bieten Dienstleistungen / Beratung
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2(b)
Beratung, Implementierung, Schulung, Audit-Tätigkeiten.

Wir bieten Managed Services / MSP
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2(b)
Betrieb der Kunden-IT im Auftrag (MSP, MSSP).

Wir nutzen, integrieren oder bieten KI-Systeme
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(d)
Bestimmt, ob KI-Lieferketten-Fragen als Nächstes erscheinen. Schließt jedes KI- / ML-Modell ein, durch das Kundendaten laufen — auch fremde LLMs über API.

2. Sicherheitspraktiken (26 Felder)

Dokumentiertes Informationssicherheits-Managementsystem (ISMS)
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.2(a)
Erforderlich nach CIR 2024/2690 §5.1.2(a) — Cybersecurity-Praktiken der Lieferanten.

ISO 27001, BSI Grundschutz oder gleichwertige Zertifizierung
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.2(b)
Erforderlich nach CIR 2024/2690 §5.1.2(b). Zertifikat über den Reiter „Zertifizierungen“ hochladen.

Jährliche Security-Awareness-Schulung für alle Mitarbeitenden
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(b)
Erforderlich nach CIR 2024/2690 §5.1.4(b) — Sensibilisierung, Fähigkeiten und Schulung.

Zuverlässigkeitsprüfung für Mitarbeitende mit Kundendaten-Zugriff
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(c)
Erforderlich nach CIR 2024/2690 §5.1.4(c) — Zuverlässigkeitsprüfung des Personals.

Dokumentierter Schwachstellen- und Patch-Management-Prozess
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(f)
Erforderlich nach CIR 2024/2690 §5.1.4(f) — Behandlung von Schwachstellen mit Risiko.

Akzeptanz des Auditrechts (oder Bereitstellung von Auditberichten)
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(e)
Erforderlich nach CIR 2024/2690 §5.1.4(e) — Auditrecht oder Bereitstellung von Auditberichten.

Einsatz von Sub-Unternehmern / Sub-Lieferanten
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(g)
Erforderlich nach CIR 2024/2690 §5.1.4(g) — Anforderungen an Unterauftragsvergabe.

Liste der Sub-Unternehmer
[text] Bedingt - Rechtsgrundlage: CIR 2024/2690 §5.1.4(g)
Listen Sie die Sub-Unternehmer und ihre Aufgaben auf. CIR 2024/2690 §5.1.4(g).

Verpflichtung zur Rückgabe / Vernichtung von Kundendaten bei Vertragsende
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(h)
Erforderlich nach CIR 2024/2690 §5.1.4(h) — Rückgabe und Vernichtung von Informationen bei Vertragsende.

Standard-Auftragsverarbeitungsvertrag (AVV) verfügbar
[boolean] Pflichtfeld - Rechtsgrundlage: GDPR Art. 28
DSGVO Art. 28 — schriftlicher Auftragsverarbeitungsvertrag.

Sicherheitsrichtlinien werden mindestens jährlich überprüft
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(a) / ENISA TIG §1.1
Erforderlich nach CIR 2024/2690 §5.1.1(c) — Sicherheitsrichtlinien müssen regelmäßig überprüft und aktualisiert werden.

Dokumentierter Notfall-/Incident-Response-Plan
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(b) / ENISA TIG §3
Erforderlich nach CIR 2024/2690 §5.1.3 / NIS2 Art. 21(2)(b) — dokumentierte Verfahren zur Behandlung von Sicherheitsvorfällen.

Dokumentierter Business-Continuity- / Disaster-Recovery-Plan
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(c) / ENISA TIG §4
Erforderlich nach CIR 2024/2690 §5.1.5 / NIS2 Art. 21(2)(c) — Aufrechterhaltung des Betriebs und Krisenmanagement.

Dokumentierte Kryptografie-Richtlinie
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(h) / ENISA TIG §9
Erforderlich nach CIR 2024/2690 §5.1.6 / NIS2 Art. 21(2)(h) — Konzepte und Verfahren zur Verwendung von Kryptografie.

Privileged Access Management (PAM) für interne Mitarbeitende
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §11.3
Erforderlich nach CIR 2024/2690 §5.1.7 / NIS2 Art. 21(2)(i) — Zugriffskontrollkonzepte für privilegierte Konten.

MFA für alle internen Admin- / privilegierten Konten erzwungen
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(j)
Erforderlich nach NIS2 Art. 21(2)(j) — Mehr-Faktor-Authentisierung für Konten mit erhöhten Rechten.

Asset-Inventar wird gepflegt
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §12.4
Erforderlich nach CIR 2024/2690 §5.1.8 / NIS2 Art. 21(2)(i) — Asset-Management.

Jährliches oder zweijährliches Penetrationstest-Programm
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(e) / ENISA TIG §6.5
Erforderlich nach CIR 2024/2690 §5.1.12 — Wirksamkeitsprüfung der Cybersicherheits-Risikomanagementmaßnahmen.

Wir legen frühere meldepflichtige Sicherheitsvorfälle auf Anfrage offen
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.1.2
ENISA TIG §5.1.2 — Auswahlkriterien verlangen, dass Einrichtungen 'die Historie des Lieferanten in Bezug auf Cybersicherheitsereignisse und Sicherheitsverletzungen' berücksichtigen.

Wir unterstützen Kunden im Vorfall ohne / zu vorab definierten Kosten
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — Verpflichtung des Lieferanten zur Unterstützung des Kunden ohne / zu vorab definierten Kosten bei einem Cyber-Vorfall durch das IKT-Produkt oder -Dienstleistung.

Vollständige Kooperation mit zuständigen Behörden (BSI, ENISA, nationale CSIRTs)
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — Verpflichtung des Lieferanten zur vollständigen Kooperation mit zuständigen Behörden bei Inspektionen, Audits und Vorfallbearbeitung.

Wir benachrichtigen Kunden über jede wesentliche Änderung der Leistungserbringung
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — Benachrichtigung über jede Entwicklung, die wesentliche Auswirkungen auf die Fähigkeit des Lieferanten zur effektiven Bereitstellung der IKT-Produkte oder -Dienstleistungen haben könnte.

Wir benachrichtigen Kunden im Voraus, wenn sich Verarbeitungsstandorte ändern
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — Benachrichtigung des Kunden im Voraus, wenn sich Verarbeitungsstandorte ändern sollen.

Dokumentierte Exit-Strategie mit verpflichtender Übergangszeit
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — Exit-Strategie mit verpflichtender angemessener Übergangszeit, IP-Bestimmungen und Verantwortlichkeiten des Lieferanten während der Exit-Phase.

Wir stellen ein SBOM-for-AI nach G7-Mindestelementen bereit
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2
G7-Cybersicherheitsbehörden (BSI, ACN, CISA u. a.) und die EU-Kommission haben am 12. Mai 2026 'Software Bill of Materials (SBOM) for Artificial Intelligence — Minimum Elements' veröffentlicht. Freiwillige Baseline-Referenz für KI-Lieferketten-Transparenz nach NIS2 Art. 21(2)(d). Umfasst sieben Cluster: Metadata, Models, Dataset Properties, Infrastructure, Security Properties, KPIs, System-Level Properties.

URL des SBOM-for-AI-Dokuments
[url] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2
Öffentliche oder kundenseitig geteilte URL zum SBOM-for-AI-Dokument des Lieferanten.

3. SaaS-spezifisch (5 Felder)

Hosting-Region
[string] Bedingt - Rechtsgrundlage: ENISA TIG §5.2
BSI IT-Grundschutz OPS.2.2 Cloud-Nutzung — wo Kundendaten gespeichert werden.

Verschlüsselung im Ruhezustand
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(h) / ENISA TIG §9
BSI IT-Grundschutz OPS.2.2.A11. AES-256 oder gleichwertig.

Verschlüsselung bei Übertragung (TLS "e 1.2)
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(h) / ENISA TIG §9
BSI IT-Grundschutz OPS.2.2.A11. Mindestens TLS 1.2, vorzugsweise TLS 1.3.

MFA für alle Admin-Konten erzwungen
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(j) / ENISA TIG §11.3
BSI IT-Grundschutz ORP.4.A23 — Zwei-Faktor-Authentisierung für privilegierte Konten.

Recovery Time Objective (RTO) in Stunden
[integer] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(c) / ENISA TIG §4
BSI IT-Grundschutz DER.4 — maximal tolerierbare Ausfallzeit für den Kundenservice.

4. On-Premise-spezifisch (4 Felder)

Bereitstellung einer Software Bill of Materials (SBOM)
[boolean] Bedingt - Rechtsgrundlage: CRA / NIS2 Art. 21(2)(d)
CRA / NIS2 Lieferketten-Transparenz. Format: CycloneDX oder SPDX.

Releases sind kryptografisch signiert
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(e) / ENISA TIG §6.5
BSI IT-Grundschutz CON.8 Software-Entwicklung — signierte Releases verhindern Lieferketten-Manipulation.

Veröffentlichte Vulnerability-Disclosure-Policy
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(e) / ENISA TIG §3
BSI IT-Grundschutz CON.10. Öffentliche security.txt oder Kontakt für Schwachstellenmeldungen.

Patch-SLA für kritische CVEs (Stunden)
[integer] Bedingt - Rechtsgrundlage: CIR 2024/2690 §5.1.4(f)
Zeit von CVE-Veröffentlichung bis zur Patch-Verfügbarkeit für kritische Schwachstellen.

5. Professional Services (3 Felder)

Umfang der Zuverlässigkeitsprüfung
[string] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(i) / CIR 2024/2690 §5.1.4(c)
BSI IT-Grundschutz ORP.2.A14 — Personalprüfung für sensible Rollen.

NDA mit allen Beratern abgeschlossen
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §11.4
BSI IT-Grundschutz ORP.2.A2 — Vertraulichkeitsvereinbarungen mit allen Beratern.

Dokumentierte Verhaltensrichtlinie auf Kundenstandort
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §11.3
BSI IT-Grundschutz ORP.3.A4 — Sicherheitssensibilisierung auf Kundenstandort.

6. Managed Services (3 Felder)

Privileged Access Management (PAM) im Einsatz
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §11.3
BSI IT-Grundschutz ORP.4.A26 — PAM für administrativen Fernzugriff.

Admin-Sitzungen werden aufgezeichnet
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(f) / ENISA TIG §10
BSI IT-Grundschutz OPS.1.2.5.A11 — aufgezeichnete Fernwartungssitzungen.

24/7-Bereitschaft
[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(b) / ENISA TIG §3
BSI IT-Grundschutz DER.2.1 — Erkennungs- und Reaktionsabdeckung für Vorfälle.