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.

1. Lieferantenprofil (18 Felder)

Firmierung (Rechtsname)

[string] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2

Der eingetragene Name Ihres Unternehmens, so wie er im Handelsregister steht. Beispiel: Müller GmbH oder Schmidt AG.

Geschäftsanschrift

[string] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2

Die Geschäftsanschrift Ihres Unternehmens. Eine Adresse genügt, auch wenn Sie mehrere Standorte haben.

Land

[country] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2

Das Land, in dem Ihr Unternehmen rechtlich sitzt. Zwei Buchstaben, zum Beispiel DE für Deutschland.

Primäre Domain

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

Ihre Hauptdomain, üblicherweise die Adresse Ihrer Webseite. Beispiel: muellergmbh.de.

Slogan (eine Zeile, kundenseitig sichtbar)

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

Eine Zeile, die Ihre Leistung zusammenfasst. Kunden sehen diese im Lieferantenprofil. Beispiel: ERP für mittelständische Produktion.

Öffentliche Beschreibung (länger)

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

Zwei bis drei Sätze über Ihr Unternehmen und Ihre Leistung. Diese Beschreibung erscheint auf Ihrem Lieferantenprofil. Verkaufsversprechen, Sicherheitspositionierung oder beides.

Beschreibung der erbrachten Leistungen

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

Ein Absatz darüber, was Ihr Unternehmen Kunden technisch liefert. Konkrete Produkte, Module oder Dienstleistungen. Vermeiden Sie reine Marketing-Sprache.

Länder / Regionen, in denen Kundendaten verarbeitet werden

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

Alle Länder, in denen Kundendaten Ihrer Kunden gespeichert oder verarbeitet werden. Komma-getrennt, ISO-Ländercodes. Beispiel: DE, NL, US. Wenn Sie ausschließlich in der EU verarbeiten, reicht eine Liste der EU-Länder.

Name des Sicherheitskontakts

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

Wer bei einem Sicherheitsvorfall direkt angesprochen wird. Bei kleineren Unternehmen oft die Geschäftsführung oder die IT-Leitung. Eine Person genügt.

E-Mail für Vorfälle

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

E-Mail-Adresse, die Kunden bei einem Sicherheitsvorfall verwenden. Idealerweise ein Verteiler wie security@firma.de, der mehrere Personen erreicht.

Telefonnummer für Vorfälle (24/7)

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

Telefonnummer für dringende Vorfallsmeldungen. Wenn Sie keinen 24/7-Bereitschaftsdienst haben, geben Sie die Geschäftszeiten in Klammern an.

Meldefrist für Vorfälle (Stunden)

[integer] Optional - Rechtsgrundlage: NIS2 Art. 23

Wie viele Stunden Sie maximal brauchen, um einen Kunden nach Erkennung eines Vorfalls zu informieren. Realistische Selbsteinschätzung, nicht Wunschwert. Übliche Werte: 24, 48 oder 72 Stunden.

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

[string] Optional - Rechtsgrundlage: ENISA TIG §5.1.2

Wenn Ihr Unternehmen selbst der NIS 2 unterliegt und beim BSI registriert ist, tragen Sie die Registrierungs-ID hier ein. Optional. Kunden sehen damit auf einen Blick, dass Sie als regulierte Einrichtung dieselbe Pflicht erfüllen.

Wir bieten SaaS / gehostete Dienste
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2(b)
Sie betreiben Software für Kunden auf eigener Infrastruktur und liefern sie über das Internet. Mehrfachauswahl möglich, wenn Sie mehrere Modelle anbieten.

Wir liefern On-Prem-Software
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2(b)
Sie liefern Software, die Ihre Kunden auf ihrer eigenen Infrastruktur installieren und betreiben.

Wir bieten Dienstleistungen / Beratung
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2(b)
Sie liefern menschliche Arbeit als Hauptleistung: Beratung, Implementierung, Schulung, Audit oder Customizing.

Wir bieten Managed Services / MSP
[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.2(b)
Sie betreiben Teile der IT-Landschaft des Kunden für ihn, mit eigenem Personal. Typisch für MSP- und MSSP-Modelle.

Wir nutzen, integrieren oder bieten KI-Systeme
[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(d)
Verarbeiten Ihre Produkte oder Dienste Kundendaten durch ein KI- oder ML-Modell? Inklusive externer Modelle, die Sie über eine API anbinden, zum Beispiel OpenAI oder Anthropic.

2. Sicherheitspraktiken (26 Felder)

Dokumentiertes Informationssicherheits-Managementsystem (ISMS)
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.2(a)
Ja, wenn Sie eine schriftliche Informationssicherheits-Richtlinie haben, klar zugewiesene Rollen, regelmäßige Überprüfungen und einen dokumentierten Umgang mit Vorfällen. ISO 27001 oder BSI Grundschutz Zertifizierung bedeutet automatisch Ja.

ISO 27001, BSI Grundschutz oder gleichwertige Zertifizierung
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.2(b)
Ja, wenn Ihr Unternehmen aktuell nach ISO 27001, BSI Grundschutz, SOC 2 Type II oder einem gleichwertigen Standard zertifiziert ist. Das Zertifikat laden Sie im Reiter Zertifizierungen hoch.

Jährliche Security-Awareness-Schulung für alle Mitarbeitenden
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(b)
Ja, wenn alle Mitarbeitenden mindestens einmal pro Jahr eine Awareness-Schulung zur Informationssicherheit erhalten. E-Learning genügt, Phishing-Simulationen kommen oben drauf.

Zuverlässigkeitsprüfung für Mitarbeitende mit Kundendaten-Zugriff
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(c)
Ja, wenn Sie für Mitarbeitende mit Zugang zu Kundendaten eine Zuverlässigkeitsprüfung durchführen. Übliche Stufe: polizeiliches Führungszeugnis oder vergleichbares Dokument bei der Einstellung.

Dokumentierter Schwachstellen- und Patch-Management-Prozess
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(f)
Ja, wenn Sie einen schriftlichen Prozess für die Behandlung von Sicherheitslücken haben: erkennen, bewerten, priorisieren, patchen oder mitigieren. CVE-Monitoring und SLA-basiertes Patching gelten als Standard.

Akzeptanz des Auditrechts (oder Bereitstellung von Auditberichten)
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(e)
Ja, wenn Sie Kunden entweder ein Auditrecht vor Ort einräumen oder ihnen stellvertretend Auditberichte (zum Beispiel SOC 2, ISAE 3402) zur Verfügung stellen.

Einsatz von Sub-Unternehmern / Sub-Lieferanten
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(g)
Ja, wenn Sie für die Leistungserbringung andere Unternehmen einsetzen, die Zugang zu Kundendaten oder Kunden-Infrastruktur haben. Typische Beispiele: AWS, Azure, Cloudflare, Stripe.

Liste der Sub-Unternehmer
[text] Bedingt - Rechtsgrundlage: CIR 2024/2690 §5.1.4(g)
Liste aller Sub-Unternehmer mit Name, Verarbeitungsstandort und Aufgabe. Eine Tabelle oder Stichpunktliste genügt. Aktualisieren Sie diese, wenn Sie einen Sub-Unternehmer hinzufügen oder entfernen.

Verpflichtung zur Rückgabe / Vernichtung von Kundendaten bei Vertragsende
[boolean] Pflichtfeld - Rechtsgrundlage: CIR 2024/2690 §5.1.4(h)
Ja, wenn Sie sich vertraglich verpflichten, Kundendaten am Ende des Vertrags zurückzugeben oder zu vernichten. Üblich: Rückgabe als Export, dann Löschung innerhalb von 30 Tagen.

Standard-Auftragsverarbeitungsvertrag (AVV) verfügbar
[boolean] Pflichtfeld - Rechtsgrundlage: GDPR Art. 28
Ja, wenn Sie einen standardisierten Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO haben, den Kunden unterschreiben können. Notwendig, sobald Sie personenbezogene Daten verarbeiten.

Sicherheitsrichtlinien werden mindestens jährlich überprüft

[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(a) / ENISA TIG §1.1

Ja, wenn Ihre Sicherheitsrichtlinien mindestens jährlich überprüft und bei Bedarf aktualisiert werden. Eine schriftliche Notiz im Dokument genügt als Nachweis.

Dokumentierter Notfall-/Incident-Response-Plan

[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(b) / ENISA TIG §3

Ja, wenn Sie einen schriftlichen Plan für den Umgang mit Sicherheitsvorfällen haben: wer entscheidet, wer kommuniziert, wer dokumentiert. Mindestens eine Tabletop-Übung pro Jahr ist gute Praxis.

Dokumentierter Business-Continuity- / Disaster-Recovery-Plan

[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(c) / ENISA TIG §4

Ja, wenn Sie einen Plan haben, der erklärt, wie Sie den Betrieb bei einem Ausfall aufrechterhalten oder schnell wiederherstellen: kritische Systeme, Ersatzwege, RTO und RPO Ziele.

Dokumentierte Kryptografie-Richtlinie

[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(h) / ENISA TIG §9

Ja, wenn Sie schriftlich festgelegt haben, welche Verschlüsselungsverfahren Sie wofür einsetzen: Daten im Transit (TLS 1.2+), Daten im Ruhezustand (AES-256), Schlüsselverwaltung, ausgewählte Hashing-Verfahren.

Privileged Access Management (PAM) für interne Mitarbeitende

[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Ja, wenn Administratoren und privilegierte Konten besondere Kontrollen haben: separater Login, MFA, Sitzungsprotokollierung oder zeitlich befristete Berechtigung.

MFA für alle internen Admin- / privilegierten Konten erzwungen

[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(j)

Ja, wenn alle internen Administrator-Konten oder Konten mit erhöhten Rechten MFA erzwingen müssen. Hardware-Tokens oder Authenticator-Apps zählen, SMS ist nicht ausreichend.

Asset-Inventar wird gepflegt

[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §12.4

Ja, wenn Sie eine aktuelle Liste aller Informationssysteme führen, die Sie für die Leistungserbringung einsetzen: Server, Datenbanken, SaaS-Werkzeuge, Endgeräte. Eine Tabelle genügt.

Jährliches oder zweijährliches Penetrationstest-Programm

[boolean] Pflichtfeld - Rechtsgrundlage: NIS2 Art. 21(2)(e) / ENISA TIG §6.5

Ja, wenn Sie mindestens alle ein bis zwei Jahre einen externen Penetrationstest beauftragen. Bei kleineren Unternehmen ist eine externe Schwachstellenanalyse als Mindestschritt akzeptabel.

Wir legen frühere meldepflichtige Sicherheitsvorfälle auf Anfrage offen

[boolean] Pflichtfeld - Rechtsgrundlage: ENISA TIG §5.1.2

Ja, wenn Sie auf Kundenanfrage offen kommunizieren, ob und welche meldepflichtigen Sicherheitsvorfälle Ihr Unternehmen in der Vergangenheit hatte. Übliche Schwelle: die letzten drei bis fünf Jahre.

Wir unterstützen Kunden im Vorfall ohne / zu vorab definierten Kosten

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

Ja, wenn Sie sich verpflichten, Kunden bei einem durch Ihr Produkt oder Ihre Dienstleistung verursachten Vorfall ohne zusätzliche Kosten zu unterstützen. Wenn Sie stattdessen einen vorab definierten Tagessatz vereinbaren, wählen Sie auch Ja.

Vollständige Kooperation mit zuständigen Behörden (BSI, ENISA, nationale CSIRTs)

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

Ja, wenn Sie sich verpflichten, mit zuständigen Behörden wie BSI, ENISA oder nationalen CSIRTs bei Inspektionen, Audits und Vorfallbearbeitung vollständig zu kooperieren. Standard für seriöse Lieferanten.

Wir benachrichtigen Kunden über jede wesentliche Änderung der Leistungserbringung

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

Ja, wenn Sie sich verpflichten, Kunden über jede wesentliche Veränderung zu informieren, die Ihre Fähigkeit zur Leistungserbringung beeinflusst: Übernahmen, Wechsel des Sub-Unternehmers, größere technische Umstellungen.

Wir benachrichtigen Kunden im Voraus, wenn sich Verarbeitungsstandorte ändern

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

Ja, wenn Sie Kunden im Voraus informieren, bevor sich der Verarbeitungsstandort ihrer Daten ändert. Wichtig für Datenschutz und für DSGVO-konforme Lieferkettenkontrolle.

Dokumentierte Exit-Strategie mit verpflichtender Übergangszeit

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

Ja, wenn Sie eine schriftliche Exit-Strategie haben: Wie lange dauert der geordnete Übergang, welche Daten und welches Wissen werden übergeben, welche Mitwirkungspflichten gelten in dieser Phase.

Wir stellen ein SBOM-for-AI nach G7-Mindestelementen bereit

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2

Optional. Ja, wenn Sie eine SBOM-for-AI nach den G7-Mindestelementen (Mai 2026) bereitstellen können. Dokumentiert Metadaten, Modelle, Trainingsdaten, Infrastruktur, Sicherheitsmerkmale, KPIs und Systemverhalten. Freiwilliger Standard.

URL des SBOM-for-AI-Dokuments

[url] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2

Öffentliche oder geteilte URL zu Ihrem SBOM-for-AI-Dokument. Kann ein PDF, eine JSON-Datei oder eine Projektseite sein.

3. SaaS-spezifisch (5 Felder)

Hosting-Region

[string] Bedingt - Rechtsgrundlage: ENISA TIG §5.2

Die Cloud-Region, in der Kundendaten gehostet werden. Beispiel: AWS eu-central-1, Azure West Europe. Geben Sie die Hauptregion an, Sekundär- oder Backup-Regionen kommen als kommagetrennte Liste dazu.

Verschlüsselung im Ruhezustand

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(h) / ENISA TIG §9

Ja, wenn Kundendaten auf der Festplatte mit AES-256 oder gleichwertig verschlüsselt sind. Cloud-verwaltete Festplattenverschlüsselung (AWS EBS, Azure Disk Encryption) zählt.

Verschlüsselung bei Übertragung (TLS "e 1.2)

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(h) / ENISA TIG §9

Ja, wenn alle kundenseitigen Endpunkte mindestens TLS 1.2 erzwingen. TLS 1.3 ist vorzuziehen. Reines HTTP muss auf HTTPS weiterleiten.

MFA für alle Admin-Konten erzwungen

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(j) / ENISA TIG §11.3

Ja, wenn jedes interne Admin-Konto auf der SaaS-Plattform MFA verwenden muss. Gleicher Standard wie für Ihre internen Admin-Vorgaben.

Recovery Time Objective (RTO) in Stunden

[integer] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(c) / ENISA TIG §4

Maximale Anzahl Stunden, die Ihr Dienst ausfallen darf, bevor die Wiederherstellung greift. Realistischer SLA-Wert, kein Wunschwert. Übliche SaaS-Werte: 4, 8 oder 24 Stunden.

4. On-Premise-spezifisch (4 Felder)

Bereitstellung einer Software Bill of Materials (SBOM)

[boolean] Bedingt - Rechtsgrundlage: CRA / NIS2 Art. 21(2)(d)

Ja, wenn Sie mit jedem Release eine Software Bill of Materials ausliefern. Standardformate: CycloneDX oder SPDX. Verpflichtend nach dem Cyber Resilience Act für Produkte, die ab Dezember 2027 auf den EU-Markt kommen.

Releases sind kryptografisch signiert

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(e) / ENISA TIG §6.5

Ja, wenn jedes Release-Artefakt eine kryptografische Signatur trägt, die Kunden prüfen können. Signaturschlüssel sind dokumentiert und werden rotiert. Sigstore- oder PGP-Signaturen zählen beide.

Veröffentlichte Vulnerability-Disclosure-Policy

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(e) / ENISA TIG §3

Ja, wenn Sie einen öffentlich dokumentierten Meldeweg für Sicherheitslücken haben. Eine security.txt-Datei auf Ihrer Domain (nach RFC 9116) oder eine dedizierte E-Mail wie security@firma.de genügt.

Patch-SLA für kritische CVEs (Stunden)

[integer] Bedingt - Rechtsgrundlage: CIR 2024/2690 §5.1.4(f)

Stunden von der öffentlichen CVE-Veröffentlichung bis zum gepatchten Release für kritische Schwachstellen (CVSS 9.0+). Realistische Zusage, kein Wunschwert. Übliche Werte: 24, 48 oder 72 Stunden.

5. Professional Services (3 Felder)

Umfang der Zuverlässigkeitsprüfung

[string] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(i) / CIR 2024/2690 §5.1.4(c)

Beschreiben Sie, wie Sie Berater für sensible Rollen prüfen. Beispiel: polizeiliches Führungszeugnis für alle Berater, zusätzlich Referenzprüfungen bei Einsätzen mit klassifizierten Daten.

NDA mit allen Beratern abgeschlossen

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §11.4

Ja, wenn jeder Berater vor dem Einsatz beim Kunden eine Vertraulichkeitsvereinbarung unterschreibt. Entweder als Bestandteil des Arbeitsvertrags oder als separates NDA.

Dokumentierte Verhaltensrichtlinie auf Kundenstandort

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Ja, wenn Sie eine schriftliche Verhaltensrichtlinie für Berater im Kundeneinsatz haben: Umgang mit Ausweisen, Sperrbildschirm-Pflicht, Verhalten beim Datenexport vom Standort.

6. Managed Services (3 Felder)

Privileged Access Management (PAM) im Einsatz

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Ja, wenn Sie für administrative Fernzugriffe auf Kundensysteme ein Privileged-Access-Management einsetzen. Beispiele: CyberArk, BeyondTrust, Teleport. Ein protokolliertes Jumphost-Setup zählt.

Admin-Sitzungen werden aufgezeichnet

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(f) / ENISA TIG §10

Ja, wenn Admin-Sitzungen auf Kundensystemen aufgezeichnet und für die Nachprüfung aufbewahrt werden. Übliche Aufbewahrung: 90 Tage bis 1 Jahr. Notwendig für forensische Rekonstruktion nach Vorfällen.

24/7-Bereitschaft

[boolean] Bedingt - Rechtsgrundlage: NIS2 Art. 21(2)(b) / ENISA TIG §3

Ja, wenn Sie eine 24/7-Bereitschaft betreiben, die auf Sicherheitsvorfälle auf Kundensystemen reagiert. Reine Unterstützung zu Geschäftszeiten qualifiziert sich nicht.