# EU-Sicherheitsfragebogen für Lieferanten

67 Fragen in 10 Abschnitten, gegliedert nach der Kritikalität des Lieferanten — der ausgehende Fragenkatalog für europäische Einkäufer. Er deckt ab, was US-amerikanische Fragebögen nicht fragen: Auftragsverarbeiterpflichten nach DSGVO Artikel 28, Lieferkettennachweise nach NIS2, Felder für IKT-Dienstleister nach DORA sowie die Exposition bei Datenstandort und CLOUD Act.

Dieses PDF ist der Begleiter zum Ausdrucken und Prüfen. Die Arbeitsdatei ist das XLSX (Lieferantenregister, Stufenrubrik, filterbarer Fragenkatalog mit Dropdowns für Antwort und Prüferbewertung); für KI-Agenten wird eine maschinenlesbare Markdown-Variante bereitgestellt. Alle drei Dateien sind kostenlos unter orbiqhq.com/templates/eu-vendor-security-questionnaire verfügbar — ohne E-Mail-Adresse.

Rechtliche Anker: DSGVO Art. 28 (Verordnung (EU) 2016/679) · NIS2 Art. 21(2)(d) (Richtlinie (EU) 2022/2555) · DORA Art. 28–30 (Verordnung (EU) 2022/2554). Diese Vorlage ist eine Hilfestellung, keine Rechtsberatung.

## So verwenden Sie den Fragebogen

**1. Stufen Sie den Lieferanten ein.** Bewerten Sie Datensensibilität, Systemzugriff, Kritikalität der Leistung (einschließlich Ihrer eigenen NIS2-/DORA-Exposition) und Ersetzbarkeit mit jeweils 1–3 Punkten. Gesamtpunktzahl 10–12 → T1 (kritisch); 7–9 → T2 (Standard); 4–6 → T3 (leicht).

**2. Wählen Sie den Fragensatz.** T3-Lieferanten beantworten die 23 mit ALLE gekennzeichneten Fragen; T2-Lieferanten beantworten 46 (ALLE + T1–T2); T1-Lieferanten beantworten alle 67, einschließlich des DORA-Zusatzes, sofern Sie ein Finanzunternehmen sind.

**3. Fordern Sie Nachweise, keine Erklärungen.** Jede Frage benennt das beizufügende Artefakt — ein Zertifikat mit Geltungsbereich, eine Managementzusammenfassung eines Penetrationstests, eine AVV-Klausel. Eine Antwort ohne Nachweis ist eine Selbstauskunft.

**4. Bewerten und dokumentieren Sie.** Kennzeichnen Sie jede Antwort mit Angemessen / Nachfassen erforderlich / Unzureichend, halten Sie offene Punkte fest und erfassen Sie das Gesamtergebnis im Lieferantenregister.

**5. Wiederholen Sie im Turnus.** T1 jährlich, T2 alle 12–18 Monate, T3 alle 2–3 Jahre — wobei Ereignisauslöser (Vorfall, Wechsel eines Unterauftragnehmers, Zertifikatsablauf) dem Kalender vorgehen.

## Warum ein europäischer Fragenkatalog

Die verbreiteten standardisierten Fragebögen stammen aus den USA: SIG (lizenzpflichtig, rund 850 Fragen im Core-Umfang) und CSA CAIQ v4 (kostenlos, 261 Fragen, Cloud-Fokus). Keiner von beiden stellt die Fragen, für die europäische Einkäufer inzwischen rechtlich einstehen müssen: ob der AVV des Lieferanten sämtliche Klauseln nach Artikel 28(3) enthält, ob eine Hosting-Option ausschließlich in der EU/im EWR besteht, ob eine US-Muttergesellschaft Daten dem Zugriff nach CLOUD Act oder FISA 702 aussetzt, ob die Fristen zur Vorfallsmeldung mit der 24-Stunden-Frühwarnung nach NIS2 Artikel 23 vereinbar sind und ob der Lieferant ein DORA-Informationsregister speisen kann. Genau diese Fragen stellt dieser Fragebogen — neben den Sicherheitsgrundlagen, die jeder Fragebogen abdecken muss.

# Fragenkatalog (67 Fragen, 10 Abschnitte)

Spalte „Stufe“: ALLE = jeder Lieferant · T1–T2 = Standard und kritisch · T1 = nur kritisch. Antwort-Enum: Ja / Teilweise / Nein / N/A — mit beigefügtem Nachweis.

## A — Unternehmen & Governance

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| A1 | Haben Sie eine benannte Sicherheitsverantwortliche Person (CISO oder gleichwertig) und eine eigene Sicherheitsfunktion? | Auszug aus dem Organigramm oder Rollenbeschreibung | ALLE |
| A2 | Führen Sie ein dokumentiertes, von der Leitung genehmigtes Richtlinienwerk zur Informationssicherheit, das mindestens jährlich überprüft wird? | Richtlinienverzeichnis mit Datum der letzten Überprüfung | ALLE |
| A3 | Verfügen Sie über ein gültiges ISO/IEC 27001:2022-Zertifikat, dessen Geltungsbereich die von uns bezogene Leistung abdeckt? | Zertifikat mit Geltungsbereichserklärung und Ablaufdatum | ALLE |
| A4 | Über welche weiteren unabhängigen Prüfnachweise verfügen Sie (SOC 2 Type II, TISAX, C5, SecNumCloud)? | Bericht oder Zertifikat; Bridge Letter, wenn der Bericht älter als 12 Monate ist | T1–T2 |
| A5 | Unterhalten Sie eine Cyber-Haftpflichtversicherung, die der Leistung angemessen ist? | Versicherungsnachweis (Deckungssumme, Laufzeit) | T1–T2 |
| A6 | Fallen Sie selbst in den Anwendungsbereich von NIS2 (wesentliche/wichtige Einrichtung) oder DORA (Finanzunternehmen / IKT-Drittdienstleister)? | Erklärung zum regulatorischen Anwendungsbereich und zu Registrierungen | T1–T2 |

## B — DSGVO & Datenschutz (Artikel 28)

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| B1 | Bieten Sie einen Auftragsverarbeitungsvertrag (AVV) an, der sämtliche Pflichtklauseln nach Artikel 28(3) enthält? | AVV-Vorlage (öffentlicher Link bevorzugt) | ALLE |
| B2 | Verarbeiten Sie personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, auch bei internationalen Datenübermittlungen? | Fundstelle der AVV-Klausel | ALLE |
| B3 | Sind alle zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet? | Fundstelle der AVV-Klausel oder Richtlinienauszug | T1–T2 |
| B4 | Führen Sie eine Dokumentation der technischen und organisatorischen Maßnahmen (TOM) im Einklang mit DSGVO Artikel 32? | TOM-Anlage oder Security-Whitepaper | ALLE |
| B5 | Veröffentlichen Sie eine aktuelle Subprozessorenliste und betreiben Sie einen Mechanismus zur Änderungsmitteilung mit Widerspruchsfrist? | URL der öffentlichen Subprozessorenseite + Beschreibung des Mitteilungsmechanismus | ALLE |
| B6 | Unterstützen Sie Kunden bei der Erfüllung von Betroffenenrechten (Auskunft, Löschung, Datenübertragbarkeit)? | Fundstelle der AVV-Klausel; Funktions- oder Prozessbeschreibung | T1–T2 |
| B7 | Sagen Sie eine Frist zur Meldung von Verletzungen des Schutzes personenbezogener Daten zu, die es dem Kunden ermöglicht, seine eigene 72-Stunden-Pflicht nach Artikel 33 einzuhalten? | Vertragliche Meldeklausel mit Stundenangabe | ALLE |
| B8 | Löschen oder übergeben Sie bei Vertragsende sämtliche personenbezogenen Daten (nach Wahl des Kunden) und löschen Sie vorhandene Kopien? | Fundstelle der AVV-Klausel; Löschverfahren | T1–T2 |

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| B9 | Gewähren Sie Prüf- und Informationsrechte nach Artikel 28(3)(h), einschließlich vom Kunden beauftragter Prüfungen durch Dritte? | Fundstelle der AVV-Klausel | T1 |
| B10 | Haben Sie, soweit erforderlich, einen Datenschutzbeauftragten oder einen EU-Vertreter (Artikel 27) benannt? | Kontaktdaten des Datenschutzbeauftragten / Vertreters | T1–T2 |

## C — Datenstandort & Datensouveränität

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| C1 | In welchen Ländern/Regionen werden Produktionsdaten und Backups gespeichert und verarbeitet? | Erklärung zum Datenstandort je Umgebung | ALLE |
| C2 | Bieten Sie eine Hosting-Option ausschließlich in der EU/im EWR an, sowohl für ruhende Daten als auch für die Verarbeitung (einschließlich Supportzugriff)? | Dokumentation zu Regionen/Bereitstellung | ALLE |
| C3 | Welcher Übermittlungsmechanismus deckt etwaige Drittlandübermittlungen ab (Angemessenheitsbeschluss, Standardvertragsklauseln, EU-US DPF)? | Verzeichnis der Übermittlungsmechanismen; Fundstellen der SCC-Module | T1–T2 |
| C4 | Unterliegt Ihre Unternehmensstruktur einem Rechtsraum außerhalb der EU (z. B. US-Muttergesellschaft), der eine Herausgabe nach dem US CLOUD Act erzwingen könnte? | Erklärung zur Unternehmensstruktur; Richtlinie zum Umgang mit behördlichen Anfragen | T1–T2 |
| C5 | Haben Sie eine Transfer-Folgenabschätzung (TIA) durchgeführt, die Zugriffe nach Art des FISA Section 702 berücksichtigt, und können Sie diese teilen? | Zusammenfassung der TIA oder Schrems-II-Analyse | T1 |
| C6 | Werden Kundendaten bei der Übertragung (TLS 1.2+) und im Ruhezustand (AES-256 oder gleichwertig) verschlüsselt? | Dokumentation der Verschlüsselungsstandards | ALLE |
| C7 | Können Verschlüsselungsschlüssel vom Kunden oder einer ausschließlich in der EU ansässigen Einheit gehalten oder kontrolliert werden (BYOK/HYOK)? | Beschreibung der Schlüsselmanagement-Architektur | T1 |
| C8 | Veröffentlichen Sie einen Transparenzbericht oder eine Richtlinie zum Umgang mit behördlichen Datenanfragen? | URL des Transparenzberichts oder Richtlinie | T1 |

## D — Zugriffskontrolle & Identität

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| D1 | Wird Multi-Faktor-Authentifizierung für sämtliche Mitarbeiterzugriffe auf Produktion und Kundendaten erzwungen? | Auszug der IAM-Richtlinie; Erklärung zur MFA-Abdeckung | ALLE |
| D2 | Unterstützen Sie SSO (SAML/OIDC) und SCIM-Provisionierung für Kundenmandanten? | Produktsicherheitsdokumentation | T1–T2 |
| D3 | Erfolgt der Zugriff auf Kundendaten rollenbasiert nach dem Least-Privilege-Prinzip, wobei der Produktionszugriff auf einen benannten Personenkreis beschränkt ist? | Zugriffskontrollrichtlinie; Rollenmatrix | ALLE |
| D4 | Werden Zugriffsrechte in einem festgelegten Turnus überprüft (bei privilegiertem Zugriff mindestens vierteljährlich)? | Jüngstes Protokoll der Zugriffsüberprüfung (geschwärzt) | T1–T2 |
| D5 | Werden privilegierte Konten über eine PAM-Lösung mit Sitzungsprotokollierung verwaltet? | Beschreibung der PAM-Werkzeuge | T1 |
| D6 | Entzieht Ihr Joiner-/Mover-/Leaver-Prozess Zugriffsrechte bei Austritt innerhalb eines festgelegten SLA? | Prozessbeschreibung mit SLA | T1–T2 |

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| D7 | Führen Sie, soweit rechtlich zulässig, Überprüfungen (Screening) von Beschäftigten mit Zugriff auf Kundendaten durch? | Erklärung zur Screening-Richtlinie | T1 |

## E — Infrastruktur & Betrieb

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| E1 | Beschreiben Sie Ihr Hosting-Modell (Cloud-Anbieter, Regionen, Single-/Multi-Tenant). | Architekturüberblick | ALLE |
| E2 | Sind Produktions-, Staging- und Entwicklungsumgebungen getrennt, ohne Kundendaten außerhalb der Produktion? | Umgebungsrichtlinie; Ansatz zur Datenmaskierung | T1–T2 |
| E3 | Betreiben Sie ein Schwachstellenmanagement-Programm mit festgelegten Behebungs-SLAs für kritische Feststellungen? | Richtlinie + Time-to-Patch-Kennzahlen der letzten 6-12 Monate | ALLE |
| E4 | Wird die Leistung mindestens jährlich von einer unabhängigen Stelle einem Penetrationstest unterzogen, und teilen Sie die Managementzusammenfassung? | Jüngste Managementzusammenfassung des Penetrationstests mit Behebungsstatus | ALLE |
| E5 | Sind Endgeräte mit EDR/Anti-Malware geschützt und Server nach einer dokumentierten Baseline gehärtet? | Beschreibung der Werkzeuge und der Baseline | T1–T2 |
| E6 | Protokollieren Sie Sicherheitsereignisse zentral und überwachen Sie diese (SIEM/SOC) mit festgelegter Aufbewahrungsdauer? | Beschreibung von Protokollierung/Monitoring; Aufbewahrungsdauer | T1–T2 |
| E7 | Wird die Infrastrukturkonfiguration als Code verwaltet bzw. einer Änderungssteuerung mit Peer Review unterworfen? | Beschreibung des Änderungsmanagement-Prozesses | T1 |
| E8 | Verfügen Sie über DDoS-Schutz und Kapazitätsmanagement für verfügbarkeitskritische Komponenten? | Erklärung zu Anbieter/Technologie | T1 |

## F — Vorfallsmanagement & Meldung

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| F1 | Führen Sie einen getesteten Incident-Response-Plan mit definierten Rollen und Schweregraden? | Zusammenfassung des IR-Plans; Datum des letzten Tests/der letzten Übung | ALLE |
| F2 | Stellen Sie Kunden einen 24/7-Kontakt für Sicherheitsvorfälle zur Verfügung? | Kontaktdaten / Eskalationspfad | ALLE |
| F3 | Welche vertragliche Frist gilt für die Benachrichtigung von Kunden über Vorfälle mit Auswirkung auf deren Leistung oder Daten (in Stunden)? | Vertragsklausel; muss mit der 24-Stunden-Frühwarnpflicht des Kunden nach NIS2 Artikel 23 vereinbar sein | ALLE |
| F4 | Für Kunden, die Finanzunternehmen sind: Können Sie deren DORA-Meldefristen für schwerwiegende Vorfälle durch rechtzeitige Informationen unterstützen? | Prozessbeschreibung mit Bezug auf DORA Artikel 19 | T1 |
| F5 | Können Sie forensische Beweismittel zu Vorfällen mit Kundenbezug sichern und bereitstellen? | Verfahren zum Umgang mit Beweismitteln | T1 |
| F6 | Stellen Sie betroffenen Kunden Nachbereitungsberichte (Ursache, Auswirkung, Korrekturmaßnahmen) zur Verfügung? | Muster oder Vorlage eines Nachbereitungsberichts | T1–T2 |

## G — Betriebskontinuität & Notfallwiederherstellung

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| G1 | Führen Sie Pläne für Betriebskontinuität und Notfallwiederherstellung, die die von uns bezogene Leistung abdecken? | Auszug aus dem BCP-/DR-Plan | ALLE |
| G2 | Welche RTO und RPO sagen Sie für die Leistung verbindlich zu? | SLA- oder DR-Dokumentation | T1–T2 |
| G3 | Sind Backups verschlüsselt, geografisch getrennt und werden sie in einem festgelegten Turnus auf Wiederherstellbarkeit getestet? | Backup-Richtlinie; Datum und Ergebnis des letzten Wiederherstellungstests | ALLE |
| G4 | Wann haben Sie Ihren DR-Plan zuletzt getestet, und mit welchem Ergebnis? | Zusammenfassung des DR-Testberichts | T1 |
| G5 | Welche kritischen Abhängigkeiten (Anbieter, Regionen, Single Points of Failure) weist die Leistung auf? | Erklärung zu Abhängigkeiten/Konzentration | T1 |

## H — Sichere Entwicklung

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| H1 | Folgen Sie einem dokumentierten sicheren Entwicklungslebenszyklus mit Sicherheitsanforderungen je Release? | Zusammenfassung der SDLC-Richtlinie | T1–T2 |
| H2 | Wird Code vor der Bereitstellung in der Produktion einem Peer Review unterzogen und gescannt (SAST/DAST/Dependency Scanning)? | Beschreibung der Security Gates in CI/CD | T1–T2 |
| H3 | Führen Sie für die Leistung eine SBOM oder ein Abhängigkeitsverzeichnis und überwachen Sie dieses auf Schwachstellen? | Erklärung zur Verfügbarkeit der SBOM (Format, Turnus) | T1 |
| H4 | Werden Secrets und Zugangsdaten in einem dedizierten Vault verwaltet (niemals in Code-Repositorys)? | Beschreibung des Secrets-Managements | T1–T2 |
| H5 | Erhalten Entwickler in einem festgelegten Turnus Schulungen zu sicherer Programmierung? | Erklärung zum Schulungsprogramm | T1 |
| H6 | Werden Sicherheitstests bei größeren Releases und Architekturänderungen durchgeführt? | Prozess für Sicherheitstests bei Releases | T1 |

## I — Unterauftragnehmer & Lieferkette

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| I1 | Führen Sie ein aktuelles Register der an der Leistungserbringung beteiligten Unterauftragnehmer mit Standorten und Rollen? | Unterauftragnehmerregister | ALLE |
| I2 | Geben Ihre Verträge mit Unterauftragnehmern gleichwertige Sicherheits- und Datenschutzpflichten weiter? | Erklärung zur Weitergabeklausel | T1–T2 |
| I3 | Bewerten Sie die Sicherheit Ihrer eigenen Lieferanten vor dem Onboarding und in einem festgelegten Turnus? | Beschreibung des Prozesses zur Lieferantenbewertung | T1–T2 |
| I4 | Werden Sie uns Änderungen bei Unterauftragnehmern vorab mitteilen und uns ein Widerspruchsrecht einräumen? | Vertragsklausel; Mitteilungsfrist | ALLE |
| I5 | Unterstützen Sie den Ausstieg des Kunden: Datenexport in einem offenen Format, Migrationsunterstützung und einen definierten Exit-Plan? | Dokumentation zu Exit/Datenportabilität (vgl. DORA Artikel 28(8) für Finanzunternehmen) | T1–T2 |

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| I6 | Können Sie Lieferantennachweise weitergeben, die wir aufgrund unserer Lieferkettenpflichten nach NIS2 Artikel 21(2)(d) anfordern? | Zusageerklärung; Prozess zur Nachweisweitergabe | T1 |

### J — Zusatz für Finanzunternehmen (DORA)

| ID | Frage | Angeforderte Nachweise | Stufe |
|---|---|---|---|
| J1 | Können Sie die Datenfelder bereitstellen, die Kunden als Finanzunternehmen für ihr DORA-Informationsregister benötigen (LEI, Dienstleistungsart, Datenstandorte)? | Feldübersicht zum Informationsregister (vgl. ITS (EU) 2024/2956) | T1 |
| J2 | Enthalten Ihre Verträge für kritische/wichtige Funktionen die Bestimmungen nach DORA Artikel 30(3) (Zugang, Prüfung, Kündigung, Ausstieg)? | Fundstellen in der Vertragsvorlage | T1 |
| J3 | Rechnen Sie mit einer Einstufung als kritischer IKT-Drittdienstleister unter DORA-Überwachung oder bereiten Sie sich darauf vor? | Erklärung | T1 |
| J4 | Werden Sie, soweit erforderlich, an den bedrohungsgeleiteten Penetrationstests (TLPT) des Kunden mitwirken? | Zusageerklärung (vgl. DORA Artikel 26-27) | T1 |
| J5 | Unterstützen Sie dokumentierte Ausstiegsstrategien einschließlich Übergangsunterstützung und Parallelbetriebsphasen? | Dokumentation der Ausstiegsstrategie | T1 |

## Vom Fragebogen zur kontinuierlichen Prüfsicherheit

Ein Fragebogen ist eine Momentaufnahme; Lieferantenrisiko ist ein Strom. Die Vendor-Assurance-Plattform von Orbiq führt dieselbe Einstufung, dieselben Fragensätze, dieselbe Nachweiserhebung und denselben Prüfworkflow kontinuierlich aus — mit KI-gestützter Bewertung der Antworten und einem Audit-Trail, der nebenbei entsteht. Mehr unter orbiqhq.com/platform/vendor-assurance-platform.

Version 1.0 · veröffentlicht am 13.07.2026 · Kostenlose Nutzung; Namensnennung willkommen. Quelle: orbiqhq.com/templates/eu-vendor-security-questionnaire