

VORLAGE · TOMORIS TOOLBOX

Lieferanten-Sicherheitsfragebogen: Vorlage für NIS2 und die Lieferkette

Fragen zu Organisation, Technik, Vorfällen und Vertragsende, mit Einstufung, Verzeichnis der Anbieter und Vertragspunkten nach DVO (EU) 2024/2690

STAND

25.10.2026

UMFANG

PDF, 8 Seiten

ONLINE

tomoris.com/downloads/lieferanten-sicherheitsfragebogen

AUF EINEN BLICK

lit. d

§ 32 Abs. 4 NISG 2026:
Sicherheit der Lieferkette

8

Vertragspunkte nach
DVO, Anhang Nr. 5.1.4

22

Fragen zum Ausfüllen in
drei Teilen

jährlich

Überprüfung des
Konzepts laut
ENISA-Hinweisen

FÜR WEN

- Einkauf und Vertragsmanagement, die IT-Dienstleister und Zulieferer auswählen
- Informationssicherheitsbeauftragte wesentlicher und wichtiger Einrichtungen
- Geschäftsführung, die für die Risikomanagementmaßnahmen verantwortlich ist
- Lieferanten, die solche Fragebögen beantworten und sich vorbereiten wollen

WORUM ES GEHT

Die Sicherheit der Lieferkette gehört zu den Mindestmaßnahmen nach § 32 NISG 2026, und die Durchführungsverordnung (EU) 2024/2690 beschreibt im Detail, was Einrichtungen bei der Auswahl, im Vertrag und in der laufenden Überprüfung ihrer Anbieter regeln müssen. Diese Vorlage übersetzt das in einen Fragebogen, den Sie IT-Dienstleistern, Softwareherstellern und Zulieferern schicken können: mit Fragen zu Organisation, Technik, Vorfällen und Vertragsende, einer Einstufung der Lieferanten nach Bedeutung, einem Verzeichnis zum Ausfüllen und den acht Vertragspunkten der DVO. Sie nutzt die Umsetzungshinweise der ENISA vom Juni 2025.

Diese Vorlage ist an Ihre Einrichtung, Ihre Lieferanten und Ihre Risiken anzupassen und ersetzt keine Rechtsberatung. Die Fragen und die Einstufung sind Empfehlungen von TOMORIS. Maßgeblich sind NISG 2026, NISV 2026 und die DVO (EU) 2024/2690 in der geltenden Fassung; für die Auftragsverarbeitung zusätzlich Art. 28 DSGVO.

Nutzung: Diese Vorlage dürfen Sie für den eigenen Gebrauch anpassen; weitergeben dürfen Sie sie nur in unveränderter Form.

INHALT

01	Was NISG 2026 und DVO verlangen	2
02	Lieferanten einstufen und erfassen	3
03	Fragebogen Teil 1: Organisation und Nachweise	4
04	Fragebogen Teil 2: Technik und Betrieb	5
05	Fragebogen Teil 3: Vorfälle, Prüfung, Vertragsende	6
06	Antworten bewerten und nachverfolgen	7
07	Vertragspunkte nach DVO Anhang Nr. 5.1.4	7
08	Quellen	8

01

Was NISG 2026 und DVO verlangen

Lieferkette als Pflichtmaßnahme und die Einzelheiten der Durchführungsverordnung

Wesentliche und wichtige Einrichtungen müssen die Sicherheit der Lieferkette regeln, einschließlich der Beziehungen zu ihren unmittelbaren Anbietern und Diensteanbietern, unter Berücksichtigung ihrer Schwachstellen, der Qualität ihrer Produkte und ihrer Cybersicherheitspraxis samt sicherer Entwicklung (§ 32 Abs. 4 lit. d NISG 2026, Art. 21 Abs. 2 lit. d und Abs. 3 NIS-2-Richtlinie). Die ENISA weist darauf hin, dass NIS2 nur die direkten Anbieter der ersten Ebene erfasst.

DVO Anhang Nr. 5.1.1 bis 5.1.3	Konzept für die Sicherheit der Lieferkette festlegen, die eigene Rolle in der Lieferkette den Anbietern mitteilen, Auswahlkriterien festlegen: Cybersicherheitsverfahren und sichere Entwicklung, Fähigkeit, Vorgaben zu erfüllen, Qualität und Resilienz der Produkte, Möglichkeit, Bezugsquellen zu streuen; soweit anwendbar die koordinierten Risikobewertungen kritischer Lieferketten der EU berücksichtigen.
DVO Anhang Nr. 5.1.4	In den Verträgen soweit angemessen acht Punkte festlegen, von Sicherheitsanforderungen über Vorfallmeldung und Prüfrecht bis zu den Pflichten bei Vertragsende (siehe Abschnitt 07).
DVO Anhang Nr. 5.1.6 und 5.1.7	Konzept überprüfen und Änderungen der Sicherheitsverfahren der Anbieter bewerten, bei wesentlichen Änderungen oder erheblichen Vorfällen; Berichte zu Leistungsvereinbarungen verfolgen, Vorfälle mit Produkten der Anbieter prüfen, außerplanmäßige Überprüfungen dokumentieren.
DVO Anhang Nr. 5.2	Verzeichnis der direkten Anbieter mit Kontaktstellen und der bereitgestellten IKT-Produkte, -Dienste und -Prozesse, laufend aktuell.
DVO Anhang Nr. 6.1.2	Beim Erwerb: Sicherheitsanforderungen, Sicherheitsupdates über die gesamte Lebensdauer, Angaben zu Hardware- und Softwarekomponenten und Sicherheitsfunktionen, Zusicherung und Nachweis der Erfüllung.
§ 2 und § 3 NISV 2026	Der Anhang der DVO gilt für alle wesentlichen und wichtigen Einrichtungen; Risiken in der IKT-Lieferkette sind eine der vier Risikokategorien, an denen sich die Risikoanalyse zumindest orientieren muss.

Welche Fragen Sie stellen und wie Sie Lieferanten einstufen, ist eine Empfehlung von TOMORIS auf Grundlage der DVO und der ENISA-Hinweise. Verpflichtend sind die Inhalte von § 32 NISG 2026 und der DVO, soweit sie für Ihre Einrichtung gelten. Für die Verarbeitung personenbezogener Daten im Auftrag braucht es zusätzlich einen Vertrag oder ein anderes Rechtsinstrument nach Art. 28 Abs. 3 DSGVO.

02

Lieferanten einstufen und erfassen

Prüfumfang nach Bedeutung des Lieferanten, Verzeichnis nach DVO Nr. 5.2

Nicht jeder Lieferant braucht denselben Aufwand. Die ENISA nennt als Kriterien unter anderem die Sensibilität der bezogenen Produkte und Dienste, die Fähigkeit des Lieferanten, die Versorgung sicherzustellen, seine Vorgeschichte bei Sicherheitsvorfällen und die Gefahr einer Abhängigkeit (Lock-in). Daraus leitet TOMORIS drei Stufen ab:

Einstufung (Empfehlung von TOMORIS)

STUFE	TYPISCHE LIEFERANTEN	PRÜFUMFANG
Hoch	Fernzugriff auf Ihre Systeme, Betrieb wichtiger Dienste, Cloud mit sensiblen Daten, IT-Dienstleister mit Administratorrechten	Ganzer Fragebogen mit Nachweisen, Vertragspunkte nach Nr. 5.1.4, jährliche Überprüfung
Mittel	Software und Geräte für wichtige Abläufe ohne dauerhaften Zugriff	Teile 1 und 2 sowie Vorfallmeldung und Vertragsende
Niedrig	Standardprodukte ohne Zugriff und ohne sensible Daten	Grundangaben im Verzeichnis, Prüfung bei Anlass

Verzeichnis der direkten Anbieter (DVO Anhang Nr. 5.2, zum Ausfüllen)

ANBIETER	KONTAKTSTELLE	PRODUKTE, DIENSTE	STUFE
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

03

Fragebogen Teil 1: Organisation und Nachweise

Wer beim Lieferanten verantwortlich ist und was er nachweisen kann

Fragebogen von [Unternehmen] an [Lieferant], ausgefüllt von [Name, Funktion] am [Datum]. Bitte beantworten Sie jede Frage und nennen Sie einen Nachweis, etwa ein Dokument, Zertifikat oder Prüfbericht.

Teil 1: Organisation

NR.	FRAGE	ANTWORT	NACHWEIS
1.1	Wer ist bei Ihnen für Informationssicherheit verantwortlich (Name, Funktion, Kontakt)?	_____	_____
1.2	Haben Sie ein dokumentiertes Sicherheitskonzept oder Managementsystem? Welche Zertifikate besitzen Sie, mit welchem Geltungsbereich und bis wann?	_____	_____
1.3	Sind Sie selbst wesentliche oder wichtige Einrichtung nach NIS2, oder fallen Ihre Produkte unter den Cyber Resilience Act?	_____	_____
1.4	Wem gehört Ihr Unternehmen, und welchem Recht unterliegen Sie?	_____	_____
1.5	Hatten Sie in den letzten drei Jahren Sicherheitsvorfälle, die Kunden betrafen? Was haben Sie daraus geändert?	_____	_____

1.6	Wie schulen Sie Ihre Mitarbeitenden in Sicherheit, und welche Qualifikationen haben die Personen, die für uns arbeiten?	_____	_____
1.7	Überprüfen Sie die Zuverlässigkeit der Mitarbeitenden, die Zugang zu unseren Systemen oder Daten haben?	_____	_____
1.8	Setzen Sie Unterauftragnehmer ein? Welche, wo, und gelten für sie dieselben Sicherheitsanforderungen?	_____	_____

Grundlagen: Auswahlkriterien und Zertifizierungen, Schulung und Zuverlässigkeitsprüfung, Unterauftragnehmer (DVO Anhang Nr. 5.1.2 und 5.1.4 lit. b, c, g); Rechtsordnung, Eigentümer, Vorgeschichte bei Vorfällen und Regulierung nach NIS2 oder Cyber Resilience Act nennt die ENISA als Kriterien.

04

Fragebogen Teil 2: Technik und Betrieb

Zugriffe, Schwachstellen, Entwicklung, Daten und Ausfallsicherheit

Teil 2: Technik und Betrieb

NR.	FRAGE	ANTWORT	NACHWEIS
2.1	Wie greifen Sie auf unsere Systeme zu? Mit persönlichen Konten, Multi-Faktor-Authentifizierung und Protokollierung?	_____	_____
2.2	Wie erfahren Sie von Schwachstellen in Ihren Produkten oder Diensten, und in welcher Frist beheben Sie sie?	_____	_____
2.3	Wie lange liefern Sie Sicherheitsupdates, und wie kündigen Sie das Supportende an?	_____	_____
2.4	Entwickeln Sie Software? Nach welchen Regeln für sichere Entwicklung und Tests?	_____	_____
2.5	Können Sie die verwendeten Hardware- und Softwarekomponenten offenlegen, etwa als Softwarestückliste (SBOM)?	_____	_____
2.6	Welche Sicherheitsfunktionen hat Ihr Produkt, und ist die sichere Konfiguration dokumentiert?	_____	_____
2.7	Wo werden unsere Daten gespeichert und verarbeitet? Melden Sie uns vorab, wenn sich das ändert?	_____	_____
2.8	Wie verschlüsseln Sie Daten bei der Übertragung und Speicherung?	_____	_____
2.9	Wie sichern Sie Daten, wie oft testen Sie die Wiederherstellung, und gibt es einen Notfallplan für Ihren Dienst?	_____	_____

Grundlagen: Sicherheitsanforderungen, Updates über die Lebensdauer, Komponenten und Sicherheitsfunktionen beim Erwerb (DVO Anhang Nr. 6.1.2), Behebung von Schwachstellen (Nr. 5.1.4 lit. f), Fernzugriff von Diensteanbietern (Nr. 6.7.2 lit. d), Multi-Faktor-Authentifizierung, Kryptografie und Aufrechterhaltung des Betriebs (§ 32 Abs. 4 lit. j, h und c NISG 2026); Speicher- und Verarbeitungsorte als Vertragsinhalt empfiehlt die ENISA.

05

Fragebogen Teil 3: Vorfälle, Prüfung, Vertragsende

Was im Ernstfall gilt und wie die Zusammenarbeit endet

Teil 3: Vorfälle und Vertrag

NR.	FRAGE	ANTWORT	NACHWEIS
3.1	Melden Sie uns Sicherheitsvorfälle, die unsere Systeme gefährden, unverzüglich? Über welchen Weg und an wen?	_____	_____
3.2	Unterstützen Sie uns bei einem Vorfall, den Ihr Produkt oder Dienst verursacht hat, und zu welchen Bedingungen?	_____	_____
3.3	Gewähren Sie ein Prüfrecht, oder stellen Sie Prüfberichte zur Verfügung?	_____	_____
3.4	Informieren Sie uns über Entwicklungen, die Ihre Leistung wesentlich beeinträchtigen könnten?	_____	_____
3.5	Was geschieht bei Vertragsende mit unseren Daten: Rückgabe, Löschung, Bestätigung? Wie unterstützen Sie den Wechsel?	_____	_____

Bestätigung

FELD	EINTRAG
Ausgefüllt von (Name, Funktion)	_____
Datum, Unterschrift	_____
Ansprechperson für Rückfragen	_____

Grundlagen: Vorfallmeldung, Prüfrecht und Pflichten bei Vertragsende (DVO Anhang Nr. 5.1.4 lit. d, e, h); Unterstützung im Vorfall, Mitteilung wesentlicher Änderungen und Ausstieg nennt die ENISA als zusätzliche Vertragsinhalte.

06 —

Antworten bewerten und nachverfolgen

Vom ausgefüllten Fragebogen zur dokumentierten Entscheidung

1

Plausibel prüfen

Antworten mit den Nachweisen abgleichen; Zertifikate auf Geltungsbereich und Gültigkeit prüfen. Fehlende Antworten nachfordern.

2

Risiko bewerten

Auswahlkriterien bei Auswahl und Vergabe berücksichtigen (DVO Nr. 5.1.5); soweit angemessen vor Vertragsabschluss eine Risikoanalyse durchführen und festhalten (ENISA zu 5.1.5).

3

Lücken schließen

Abweichungen über Vertragsklauseln, Leistungsvereinbarungen oder eigene Schutzmaßnahmen auffangen, etwa eingeschränkte Zugriffe. Ist das nicht möglich, Alternativen prüfen.

4

Entscheiden und dokumentieren

Freigabe, Auflagen oder Ablehnung mit Begründung und Verantwortlichen festhalten; Lieferant im Verzeichnis eintragen.

5

Laufend überwachen

Leistungsberichte verfolgen, Vorfälle mit Produkten des Lieferanten prüfen, die Notwendigkeit außerplanmäßiger Überprüfungen prüfen (DVO Anhang Nr. 5.1.7), etwa bei Vorfällen, wesentlichen Änderungen oder Vertragsverletzungen (ENISA); das Konzept laut ENISA mindestens jährlich überprüfen.

Für die Selbstdeklaration an die Cybersicherheitsbehörde sind insbesondere Informationen zur Sicherheit der Lieferketten zu übermitteln (§ 33 Abs. 1 NISG 2026). Ausgefüllte Fragebögen, Bewertungen und das Verzeichnis sind dafür eine gute Grundlage.

07 —

Vertragspunkte nach DVO Anhang Nr. 5.1.4

Was Verträge mit Anbietern soweit angemessen festlegen

- ☐ a) Cybersicherheitsanforderungen an den Anbieter, einschließlich der Anforderungen beim Erwerb nach Nummer 6.1.
- ☐ b) Anforderungen an Sensibilisierung, Qualifikation und Ausbildung sowie gegebenenfalls Zertifizierungen der Mitarbeitenden des Anbieters.
- ☐ c) Anforderungen an die Zuverlässigkeitsüberprüfung der Mitarbeitenden des Anbieters.

- ☐ d) Pflicht, Sicherheitsvorfälle, die ein Risiko für Ihre Systeme darstellen, unverzüglich zu melden.
- ☐ e) Recht auf Prüfung oder auf Erhalt von Prüfberichten.
- ☐ f) Pflicht zur Behebung von Schwachstellen, die ein Risiko für Ihre Systeme darstellen.
- ☐ g) Regeln für Unteraufträge; wenn zulässig, Sicherheitsanforderungen an Unterauftragnehmer.
- ☐ h) Pflichten bei Vertragsende, etwa Rückgabe und Entsorgung erlangter Informationen.

Bei großen Anbietern, deren Verträge sich kaum verhandeln lassen, nennt die ENISA Auswege: gemeinsamer Einkauf mit ähnlichen Organisationen, Vertretung über einen Verband, Anbieter mit veröffentlichten Sicherheitszusagen oder anerkannten Zertifizierungen, Vertragsmuster öffentlicher Stellen und eine kurze Liste von Alternativen.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck
tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen
tomoris.com/contact
contact@tomoris.com

08

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§ 32 Abs. 4 lit. c, d, h, j und § 33 Abs. 1, gelesen am 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 2 **Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), deutsche Fassung auf EUR-Lex**
Art. 21 Abs. 2 lit. d und Abs. 3, gelesen am 25.10.2026
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- 3 **Durchführungsverordnung (EU) 2024/2690, deutsche Fassung auf EUR-Lex**
Anhang Nr. 5.1, 5.2, 6.1.2 und 6.7.2, gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- 4 **NISV 2026, BGBl. II Nr. 290/2026**
§ 2 Anwendbarkeit der DVO, § 3 Risikokategorien, gelesen am 25.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 5 **DSGVO, deutsche Fassung auf EUR-Lex**
Art. 28 Abs. 3, gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 6 **ENISA: Technical Implementation Guidance, Version 1.0 (Juni 2025)**
Kapitel 5 Supply Chain Security, gelesen am 25.10.2026
www.enisa.europa.eu/publications/nis2-technical-implementation-...
- 7 **ENISA: Good Practices for Supply Chain Cybersecurity (Juni 2023)**
Executive Summary und Abschnitt 2.1, gelesen am 25.10.2026
www.enisa.europa.eu/publications/good-practices-for-supply-chai...