NIS 2 Supplier Questionnaire

An open, EU-anchored questionnaire for NIS 2 supplier due diligence

Version 3.1.0 - Last updated 2026-05-15 - 59 fields across 6 sections

Every field is anchored to an EU-level primary source: NIS 2 Art. 21(2), CIR 2024/2690, ENISA Technical Implementation Guidance, GDPR Art. 28, or the Cyber Resilience Act. Sector overlays (TISAX, VDA ISA, BSI C5, KRITIS) sit on top of this baseline.

1. Supplier Profile (18 fields)

Legal name

[string] Required - Legal basis: ENISA TIG §5.2

Required by CIR 2024/2690 §5.2(a) — supplier register entry.

Registered address

[string] Required - Legal basis: ENISA TIG §5.2

Required by CIR 2024/2690 §5.2(a) — supplier register entry.

Country

[country] Required - Legal basis: ENISA TIG §5.2

ISO 3166-1 alpha-2 code, e.g. DE, FR, IT.

Primary domain

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

The supplier's primary public domain.

Tagline (one line, customer-facing)

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

Short summary shown to customers.

Public description (longer)

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

Longer description of the supplier.

Description of services provided

[text] Required - Legal basis: ENISA TIG §5.2(b) + §5.1.4 TIPS

Required by ENISA TIG §5.2(b) + §5.1.4 TIPS — clear and complete description of the ICT products and services you provide. One paragraph.

Countries / regions where customer data is processed

[string] Required - Legal basis: ENISA TIG §5.1.4 TIPS

Required by ENISA TIG §5.1.4 TIPS — list every country / region where your customers' data is produced, processed or stored. Comma-separated.

Security contact name

[string] Required - Legal basis: CIR 2024/2690 §5.1.4(d)

Required by CIR 2024/2690 §5.1.4(d) — incident notification chain.

Incident contact email

[email] Required - Legal basis: CIR 2024/2690 §5.1.4(d)

Default email used by customers for incident notifications.

Incident contact phone (24/7)

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

24/7 phone for critical incident notifications.

Incident notification SLA (hours)

[integer] Optional - Legal basis: NIS2 Art. 23

Maximum time from incident detection to customer notification.

BSI registration ID (only if your company is itself NIS2-regulated)

[string] Optional - Legal basis: ENISA TIG §5.1.2

Optional. ENISA TIG §5.1.2 — if your company is itself a NIS2-regulated entity with a BSI registration, your customers can use this fact to satisfy their §5.1.2 supplier-selection criteria.

We provide SaaS / hosted services

[boolean] Required - Legal basis: ENISA TIG §5.2(b)

Determines which technical questions you'll see next. Pick all that apply.

We deliver on-prem software

[boolean] Required - Legal basis: ENISA TIG §5.2(b)

Software your customers install on their own hardware.

We provide professional services / consulting
[boolean] Required - Legal basis: ENISA TIG §5.2(b)
Consulting, implementation, training, audit work.

We provide managed services / MSP
[boolean] Required - Legal basis: ENISA TIG §5.2(b)
Operating the customer's IT under contract (MSP, MSSP).

We use, integrate or provide AI systems
[boolean] Required - Legal basis: NIS2 Art. 21(2)(d)
Determines whether AI supply-chain disclosure questions appear next. Includes any AI / ML model the customer's data passes through, including third-party LLMs accessed via API.

2. Security Practices (26 fields)

Documented Information Security Management System (ISMS)
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.2(a)
Required by CIR 2024/2690 §5.1.2(a) — cybersecurity practices of suppliers.

Hold ISO 27001, BSI Grundschutz, or equivalent certification
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.2(b)
Required by CIR 2024/2690 §5.1.2(b). Upload the certificate via the Certifications tab.

Annual security awareness training for all staff
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(b)
Required by CIR 2024/2690 §5.1.4(b) — awareness, skills and training.

Background checks on staff with customer data access
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(c)
Required by CIR 2024/2690 §5.1.4(c) — verification of staff background.

Documented vulnerability handling and patching process
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(f)
Required by CIR 2024/2690 §5.1.4(f) — handle vulnerabilities that present a risk.

Accept customer right to audit (or provide audit reports)
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(e)
Required by CIR 2024/2690 §5.1.4(e) — right to audit or to receive audit reports.

Use subprocessors / sub-suppliers
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(g)
Required by CIR 2024/2690 §5.1.4(g) — subcontracting requirements.

List of subprocessors
[text] Conditional - Legal basis: CIR 2024/2690 §5.1.4(g)
List the subprocessors and what they do for you. CIR 2024/2690 §5.1.4(g).

Commit to return / destroy customer data on termination
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(h)
Required by CIR 2024/2690 §5.1.4(h) — retrieval and disposal of information at termination.

Standard data processing agreement (DPA) available
[boolean] Required - Legal basis: GDPR Art. 28
GDPR Art. 28 — written data processing agreement.

Security policies reviewed at least annually
[boolean] Required - Legal basis: NIS2 Art. 21(2)(a) / ENISA TIG §1.1
Required by CIR 2024/2690 §5.1.1(c) — security policies must be reviewed and updated regularly.

Documented incident response plan
[boolean] Required - Legal basis: NIS2 Art. 21(2)(b) / ENISA TIG §3
Required by CIR 2024/2690 §5.1.3 / NIS2 Art. 21(2)(b) — documented incident handling procedures.

Documented business continuity / disaster recovery plan
[boolean] Required - Legal basis: NIS2 Art. 21(2)(c) / ENISA TIG §4
Required by CIR 2024/2690 §5.1.5 / NIS2 Art. 21(2)(c) — business continuity and crisis management.

Documented cryptography policy
[boolean] Required - Legal basis: NIS2 Art. 21(2)(h) / ENISA TIG §9
Required by CIR 2024/2690 §5.1.6 / NIS2 Art. 21(2)(h) — policies and procedures regarding the use of cryptography.

Privileged access management (PAM) for internal staff
[boolean] Required - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §11.3
Required by CIR 2024/2690 §5.1.7 / NIS2 Art. 21(2)(i) — access control policies for privileged accounts.

MFA enforced for all internal admin / privileged accounts
[boolean] Required - Legal basis: NIS2 Art. 21(2)(j)
Required by NIS2 Art. 21(2)(j) — multi-factor authentication for accounts with elevated privileges.

Maintain an inventory of information assets
[boolean] Required - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §12.4
Required by CIR 2024/2690 §5.1.8 / NIS2 Art. 21(2)(i) — asset management.

Annual or biennial penetration testing program
[boolean] Required - Legal basis: NIS2 Art. 21(2)(e) / ENISA TIG §6.5
Required by CIR 2024/2690 §5.1.12 — testing of cybersecurity risk-management measures.

We disclose past notifiable cybersecurity events when asked by customers
[boolean] Required - Legal basis: ENISA TIG §5.1.2
ENISA TIG §5.1.2 — selection criteria require entities to consider 'the supplier's history in relation to cybersecurity events and breaches'.

Provide incident assistance to customers at no / ex-ante cost
[boolean] Required - Legal basis: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — supplier obligation to assist the customer at no / ex-ante cost during a cyber incident caused by the ICT product or service.

Fully cooperate with competent authorities (BSI, ENISA, national CSIRTs)
[boolean] Required - Legal basis: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — supplier obligation to fully cooperate with competent authorities during inspections, audits and incident handling.

Notify customers of any material change affecting service delivery
[boolean] Required - Legal basis: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — notification of any development that might have a material impact on the supplier's ability to effectively provide the ICT products or services.

Notify customers in advance if data-processing locations change
[boolean] Required - Legal basis: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — notify the customer in advance if data-processing locations envisaged to change.

Documented exit strategy with mandatory transition period
[boolean] Required - Legal basis: ENISA TIG §5.1.4 TIPS
ENISA TIG §5.1.4 TIPS — exit strategy with a mandatory adequate transition period, IP provisions and supplier responsibilities during the exit period.

Provide an SBOM-for-AI per G7 minimum elements
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2
G7 cybersecurity authorities (BSI, ACN, CISA et al.) and the EU Commission published 'Software Bill of Materials (SBOM) for Artificial Intelligence — Minimum Elements' on 12 May 2026. Voluntary baseline reference for AI supply-chain transparency under NIS2 Art. 21(2)(d). Covers seven clusters: metadata, models, dataset properties, infrastructure, security properties, KPIs, system-level properties.

SBOM-for-AI document URL
[url] Conditional - Legal basis: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2
Public or customer-shared URL pointing to the supplier's SBOM-for-AI document.

3. SaaS-specific (5 fields)

Hosting region
[string] Conditional - Legal basis: ENISA TIG §5.2
BSI IT-Grundschutz OPS.2.2 Cloud-Nutzung — where customer data is stored.

Encryption at rest
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(h) / ENISA TIG §9
BSI IT-Grundschutz OPS.2.2.A11. AES-256 or equivalent.

Encryption in transit (TLS "e 1.2)
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(h) / ENISA TIG §9
BSI IT-Grundschutz OPS.2.2.A11. TLS 1.2 minimum, TLS 1.3 preferred.

MFA enforced for all admin accounts
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(j) / ENISA TIG §11.3
BSI IT-Grundschutz ORP.4.A23 — second-factor authentication for privileged accounts.

Recovery time objective (RTO) in hours
[integer] Conditional - Legal basis: NIS2 Art. 21(2)(c) / ENISA TIG §4
BSI IT-Grundschutz DER.4 — maximum tolerated downtime for customer service.

4. On-Premise-specific (4 fields)

Provide a Software Bill of Materials (SBOM)
[boolean] Conditional - Legal basis: CRA / NIS2 Art. 21(2)(d)
CRA / NIS2 supply-chain transparency. Format: CycloneDX or SPDX.

Releases are cryptographically signed
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(e) / ENISA TIG §6.5
BSI IT-Grundschutz CON.8 Software-Entwicklung — signed releases prevent supply-chain tampering.

Published vulnerability disclosure policy
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(e) / ENISA TIG §3
BSI IT-Grundschutz CON.10. Public security.txt or contact for vulnerability reports.

Patch SLA for critical CVEs (hours)
[integer] Conditional - Legal basis: CIR 2024/2690 §5.1.4(f)
Time from CVE disclosure to patch availability for critical vulnerabilities.

5. Professional Services (3 fields)

Background check scope
[string] Conditional - Legal basis: NIS2 Art. 21(2)(i) / CIR 2024/2690 §5.1.4(c)
BSI IT-Grundschutz ORP.2.A14 — staff vetting for sensitive roles.

NDA in place with all consultants
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §11.4
BSI IT-Grundschutz ORP.2.A2 — confidentiality agreements with all consultants.

Documented customer-premises behaviour policy
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §11.3
BSI IT-Grundschutz ORP.3.A4 — security awareness on customer premises.

6. Managed Services (3 fields)

Privileged access management (PAM) in place
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §11.3
BSI IT-Grundschutz ORP.4.A26 — PAM for administrative remote access.

Admin sessions are recorded
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(f) / ENISA TIG §10
BSI IT-Grundschutz OPS.1.2.5.A11 — recorded remote maintenance sessions.

24/7 on-call coverage
[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(b) / ENISA TIG §3
BSI IT-Grundschutz DER.2.1 — incident detection and response coverage.