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.

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

1. Supplier Profile (18 fields)

Legal name

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

Your company's registered name, as it appears in the commercial register. Example: Müller GmbH or Acme Software Ltd.

Registered address

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

Your company's registered business address. One address is enough, even if you have several locations.

Country

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

The country where your company is legally established. Two letters, e.g. DE for Germany.

Primary domain

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

Your main domain, usually the URL of your website. Example: acmesoftware.com.

Tagline (one line, customer-facing)

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

One line summarising what you offer. Customers see this on your supplier profile. Example: ERP for SME manufacturing.

Public description (longer)

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

Two to three sentences about your company and what you do. This appears on your supplier profile. Sales pitch, security posture, or both.

Description of services provided

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

One paragraph on what your company technically delivers to customers. Concrete products, modules, or services. Avoid pure marketing language.

Countries / regions where customer data is processed

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

Every country where your customers' data is stored or processed. Comma-separated, ISO country codes. Example: DE, NL, US. If you process entirely within the EU, listing the EU countries is enough.

Security contact name

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

Who customers contact when a security incident hits. In smaller companies often the managing director or IT lead. One person is enough.

Incident contact email

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

Email address customers use to report a security incident. Ideally a distribution list like security@example.com that reaches multiple people.

Incident contact phone (24/7)

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

Phone number for urgent incident reports. If you do not run 24/7 on-call, mention your business hours in brackets.

Incident notification SLA (hours)

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

Hours from incident detection to customer notification, at the latest. Realistic self-assessment, not aspirational. Common values: 24, 48, or 72 hours.

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

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

If your company is itself NIS 2 regulated and registered with the BSI, enter the registration ID here. Optional. Lets customers see at a glance that you meet the same obligation as a regulated entity.

We provide SaaS / hosted services

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

You run software for customers on your own infrastructure and deliver it over the internet. Tick more than one box if you offer several models.

We deliver on-prem software
[boolean] Required - Legal basis: ENISA TIG §5.2(b)
You deliver software that customers install and run on their own infrastructure.

We provide professional services / consulting
[boolean] Required - Legal basis: ENISA TIG §5.2(b)
Your main deliverable is human work: consulting, implementation, training, audit, or customisation.

We provide managed services / MSP
[boolean] Required - Legal basis: ENISA TIG §5.2(b)
You operate parts of your customer's IT for them, with your own staff. Typical for MSP and MSSP models.

We use, integrate or provide AI systems
[boolean] Required - Legal basis: NIS2 Art. 21(2)(d)
Do your products or services process customer data through an AI or ML model? Includes external models you call through an API, for example OpenAI or Anthropic.

2. Security Practices (26 fields)

Documented Information Security Management System (ISMS)
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.2(a)
Tick yes if you have a written information security policy with assigned roles, regular reviews, and documented incident handling. ISO 27001 or BSI Grundschutz certification implies yes.

Hold ISO 27001, BSI Grundschutz, or equivalent certification
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.2(b)
Tick yes if your company currently holds an ISO 27001, BSI Grundschutz, SOC 2 Type II, or equivalent certification. Upload the certificate in the Certifications tab.

Annual security awareness training for all staff
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(b)
Tick yes if every staff member receives at least one annual information-security awareness training. E-learning counts; phishing simulations add to it.

Background checks on staff with customer data access
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(c)
Tick yes if you run a background check for staff with access to customer data. Common bar: a criminal record extract or equivalent document on hire.

Documented vulnerability handling and patching process
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(f)
Tick yes if you have a written process for handling security vulnerabilities: detect, assess, prioritise, patch or mitigate. CVE monitoring and SLA-driven patching are the standard.

Accept customer right to audit (or provide audit reports)
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(e)
Tick yes if you either grant customers an on-site audit right or provide substitute audit reports (for example SOC 2, ISAE 3402).

Use subprocessors / sub-suppliers
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(g)
Tick yes if you use other companies to deliver your service that have access to customer data or infrastructure. Typical examples: AWS, Azure, Cloudflare, Stripe.

List of subprocessors
[text] Conditional - Legal basis: CIR 2024/2690 §5.1.4(g)
List every subprocessor with name, processing location, and what they do for you. A table or bullet list is enough. Update whenever you add or remove one.

Commit to return / destroy customer data on termination
[boolean] Required - Legal basis: CIR 2024/2690 §5.1.4(h)
Tick yes if you contractually commit to returning or destroying customer data at the end of the contract. Common practice: export and return, then delete within 30 days.

Standard data processing agreement (DPA) available
[boolean] Required - Legal basis: GDPR Art. 28
Tick yes if you have a standard data processing agreement under GDPR Article 28 that customers can sign. Required as soon as you process personal data.

Security policies reviewed at least annually
[boolean] Required - Legal basis: NIS2 Art. 21(2)(a) / ENISA TIG §1.1
Tick yes if your security policies are reviewed at least once a year and updated as needed. A written note in the document is enough evidence.

Documented incident response plan

[boolean] Required - Legal basis: NIS2 Art. 21(2)(b) / ENISA TIG §3

Tick yes if you have a written plan for handling security incidents: who decides, who communicates, who documents. At least one tabletop exercise per year is good practice.

Documented business continuity / disaster recovery plan

[boolean] Required - Legal basis: NIS2 Art. 21(2)(c) / ENISA TIG §4

Tick yes if you have a plan that explains how you keep running or recover quickly during an outage: critical systems, fallbacks, RTO and RPO targets.

Documented cryptography policy

[boolean] Required - Legal basis: NIS2 Art. 21(2)(h) / ENISA TIG §9

Tick yes if you have written down which cryptography you use where: data in transit (TLS 1.2+), data at rest (AES-256), key management, hashing algorithms.

Privileged access management (PAM) for internal staff

[boolean] Required - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Tick yes if administrators and privileged accounts get extra controls: separate sign-in, MFA, session logging, or just-in-time access.

MFA enforced for all internal admin / privileged accounts

[boolean] Required - Legal basis: NIS2 Art. 21(2)(j)

Tick yes if every internal admin or privileged account must use MFA. Hardware tokens or authenticator apps count; SMS does not.

Maintain an inventory of information assets

[boolean] Required - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §12.4

Tick yes if you keep a current list of every information system you use to deliver your service: servers, databases, SaaS tools, endpoints. A spreadsheet is enough.

Annual or biennial penetration testing program

[boolean] Required - Legal basis: NIS2 Art. 21(2)(e) / ENISA TIG §6.5

Tick yes if you commission an external penetration test at least every one to two years. For smaller companies, an external vulnerability scan as a minimum step is acceptable.

We disclose past notifiable cybersecurity events when asked by customers

[boolean] Required - Legal basis: ENISA TIG §5.1.2

Tick yes if, on customer request, you openly disclose whether and which reportable security incidents your company had in the past. Common window: the last three to five years.

Provide incident assistance to customers at no / ex-ante cost

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

Tick yes if you commit to helping customers at no extra cost when an incident is caused by your product or service. If you agree a pre-defined day rate up front instead, also tick yes.

Fully cooperate with competent authorities (BSI, ENISA, national CSIRTs)

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

Tick yes if you commit to fully cooperating with competent authorities like BSI, ENISA, or national CSIRTs during inspections, audits, and incident handling. Standard for serious suppliers.

Notify customers of any material change affecting service delivery

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

Tick yes if you commit to notifying customers of any material change affecting your ability to deliver: acquisitions, subprocessor changes, major technical shifts.

Notify customers in advance if data-processing locations change

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

Tick yes if you notify customers in advance before the processing location of their data changes. Important for data protection and for GDPR-compliant supply chain oversight.

Documented exit strategy with mandatory transition period

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

Tick yes if you have a written exit strategy: how long an orderly handover takes, what data and knowledge gets transferred, what you commit to during the transition.

Provide an SBOM-for-AI per G7 minimum elements

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2

Optional. Tick yes if you can provide an SBOM-for-AI per the G7 minimum elements (May 2026). Documents metadata, models, training data, infrastructure, security properties, KPIs, and system behaviour. Voluntary standard.

SBOM-for-AI document URL

[url] Conditional - Legal basis: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2

Public or shared URL to your SBOM-for-AI document. Can be a PDF, a JSON file, or a project page.

3. SaaS-specific (5 fields)

Hosting region

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

The cloud region where customer data is hosted. Example: AWS eu-central-1, Azure West Europe. Name the primary region; secondary or backup regions can be added comma-separated.

Encryption at rest

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(h) / ENISA TIG §9

Tick yes if customer data on disk is encrypted at rest with AES-256 or equivalent. Cloud-managed disk encryption (AWS EBS, Azure Disk Encryption) counts.

Encryption in transit (TLS "e 1.2)

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(h) / ENISA TIG §9

Tick yes if all customer-facing endpoints enforce TLS 1.2 or higher. TLS 1.3 is preferred. Plain HTTP must redirect to HTTPS.

MFA enforced for all admin accounts

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(j) / ENISA TIG §11.3

Tick yes if every internal admin account on the SaaS platform must use MFA. Same standard as your internal admin policy.

Recovery time objective (RTO) in hours

[integer] Conditional - Legal basis: NIS2 Art. 21(2)(c) / ENISA TIG §4

Maximum number of hours your service can be unavailable before recovery. Realistic SLA value, not aspirational. Common SaaS values: 4, 8, or 24 hours.

4. On-Premise-specific (4 fields)

Provide a Software Bill of Materials (SBOM)

[boolean] Conditional - Legal basis: CRA / NIS2 Art. 21(2)(d)

Tick yes if you ship a Software Bill of Materials with every release. CycloneDX or SPDX are the standard formats. Mandatory under the Cyber Resilience Act for products placed on the EU market from December 2027.

Releases are cryptographically signed

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(e) / ENISA TIG §6.5

Tick yes if every release artefact carries a cryptographic signature customers can verify. Signing keys are documented and rotated. Sigstore or PGP signatures both count.

Published vulnerability disclosure policy

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(e) / ENISA TIG §3

Tick yes if you have a publicly documented way to report security vulnerabilities. A security.txt file under your domain (per RFC 9116) or a dedicated email like security@example.com is enough.

Patch SLA for critical CVEs (hours)

[integer] Conditional - Legal basis: CIR 2024/2690 §5.1.4(f)

Hours from public CVE disclosure to a patched release for critical vulnerabilities (CVSS 9.0+). Realistic commitment, not aspirational. Common values: 24, 48, or 72 hours.

5. Professional Services (3 fields)

Background check scope

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

Describe how you vet consultants for sensitive roles. Example: criminal record extract for all consultants, plus reference checks for engagements involving classified data.

NDA in place with all consultants

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §11.4

Tick yes if every consultant signs a confidentiality agreement before being assigned to customer work. Either as part of the employment contract or as a separate NDA.

Documented customer-premises behaviour policy

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Tick yes if you have a written code of conduct for consultants working on customer premises: badge handling, locked-screen rule, what to do if data leaves the site.

6. Managed Services (3 fields)

Privileged access management (PAM) in place

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Tick yes if you use a privileged access management tool for administrative remote sessions on customer systems. Examples: CyberArk, BeyondTrust, Teleport. A logged jump-host setup counts.

Admin sessions are recorded

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(f) / ENISA TIG §10

Tick yes if admin sessions on customer systems are recorded and retained for review. Common retention: 90 days to 1 year. Needed for forensic reconstruction after incidents.

24/7 on-call coverage

[boolean] Conditional - Legal basis: NIS2 Art. 21(2)(b) / ENISA TIG §3

Tick yes if you operate a 24/7 on-call rotation that responds to security incidents on customer systems. Business-hours-only support does not qualify.

License: MIT (schema) + CC BY 4.0 (content). Free to use, fork, and adapt.