NIS 2 ART. 21(2)(D)

NIS 2 Supplier Questionnaire

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

Supplier profile	16 fields
Security practices	31 fields
Software as a service (SaaS)	2 fields
Software on the customer's premises (on-premise)	4 fields

Every question names its EU-level source: Implementing Regulation (EU) 2024/2690, ENISA's Technical Implementation Guidance, the GDPR or the Cyber Resilience Act. Where it serves ISO/IEC 27001:2022 Annex A controls, they are listed beside it. Every supplier answers 21 questions; each of the others states the answer it depends on. That follows from what the supplier reaches at its customers: their data, their systems, their premises, or software it runs or ships. 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)

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

1. Supplier profile

16 fields

Legal name

STRING · REQUIRED · LEGAL BASIS: CIR 2024/2690 §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: CIR 2024/2690 §5.2

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

Country

COUNTRY · REQUIRED · LEGAL BASIS: CIR 2024/2690 §5.2

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

Primary domain

DOMAIN · OPTIONAL · LEGAL BASIS: CIR 2024/2690 §5.2(A)

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

Description of services provided

TEXT · REQUIRED · LEGAL BASIS: CIR 2024/2690 §5.2(B) · ISO/IEC 27001:2022 A.5.19, A.5.22

One paragraph on what you deliver to customers: concrete products, services or work, not marketing. Examples: “Office cleaning three evenings a week, with keys to the building” or “Payroll accounting for up to 200 employees”.

Security contact name

STRING · REQUIRED · LEGAL BASIS: CIR 2024/2690 §5.2(A) · ISO/IEC 27001:2022 A.5.20, A.5.24

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 §5.2(A) · ISO/IEC 27001:2022 A.5.20, A.5.24

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

Incident contact phone

PHONE · OPTIONAL · LEGAL BASIS: CIR 2024/2690 §5.2(A) · ISO/IEC 27001:2022 A.5.20, A.5.24

Phone number for urgent incident reports. Add the hours it is answered in brackets; round-the-clock cover is not expected.

How fast you inform customers of an incident (hours)

INTEGER · OPTIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(D) · ISO/IEC 27001:2022 A.5.20, A.5.24

At most this many hours after you notice a security incident that affects a customer, for example a data leak, a hacked account or a lost key. A customer under NIS 2 must send its authority an early warning within 24 hours of becoming aware of a significant incident (Art. 23(4)(a) NIS 2), so a promise of 24 hours or less helps them most. Give a value you keep.

We provide SaaS / hosted services

BOOLEAN · REQUIRED · LEGAL BASIS: CIR 2024/2690 §5.2(B) · ISO/IEC 27001:2022 A.5.19, A.5.22, A.5.23

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: CIR 2024/2690 §5.2(B) · ISO/IEC 27001:2022 A.5.19, A.5.22

You deliver software that customers install and run on their own infrastructure.

We provide managed services / MSP

BOOLEAN · REQUIRED · LEGAL BASIS: CIR 2024/2690 §5.2(B) · ISO/IEC 27001:2022 A.5.19, A.5.22

You operate parts of your customer's IT for them, with your own staff. Typical for MSP and MSSP models.

We process or store our customers' data

BOOLEAN · REQUIRED · LEGAL BASIS: ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.19

Tick yes if you hold or handle your customers' data or documents, electronically or on paper, for example in software, a data centre, a ticket system, accounting or an archive.

Countries / regions where customer data is processed

STRING · CONDITIONAL · LEGAL BASIS: ENISA TIG §5.1.4 TIPS · ISO/IEC 27001:2022 A.5.20, A.5.23, A.5.34

Only if: We process or store our customers' data = Yes

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.

We access our customers' systems

BOOLEAN · REQUIRED · LEGAL BASIS: ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.19

Tick yes if you can sign in to your customers' systems, remotely, as an administrator or on site, for example for maintenance, support or operations.

Our staff enter our customers' premises

BOOLEAN · REQUIRED · LEGAL BASIS: CIR 2024/2690 §11.1.2(A); §13.3.2(B) · ISO/IEC 27001:2022 A.5.19

Tick yes if your staff or subcontractors go into a customer's offices or buildings, escorted or not, for example for cleaning, maintenance, repairs, deliveries into the building or on-site support. Holding keys, badges or door codes counts.

2. Security practices

31 fields

Staff who work for customers are instructed in security when they start and at regular intervals

BOOLEAN · REQUIRED · LEGAL BASIS: CIR 2024/2690 §5.1.4(B) · ISO/IEC 27001:2022 A.6.3

Tick yes if everyone who works for customers learns the security rules that apply to them when they start, and again at regular intervals, for example in a short briefing, an e-learning course or written rules they sign.

We accept audits by customers or provide audit reports

BOOLEAN · REQUIRED · LEGAL BASIS: CIR 2024/2690 §5.1.4(E) · ISO/IEC 27001:2022 A.5.20, A.5.22

Tick yes if you either let customers audit you or give them audit reports instead (for example SOC 2, ISAE 3402).

We use subcontractors to deliver our service

BOOLEAN · REQUIRED · LEGAL BASIS: CIR 2024/2690 §5.1.4(G) · ISO/IEC 27001:2022 A.5.20, A.5.21

Tick yes if other companies help you deliver your service and in doing so reach customer data, systems or premises. Examples: a cloud host such as AWS or Azure, a payment provider, or a subcontracted crew that works on site.

List of subcontractors

TEXT · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(G) · ISO/IEC 27001:2022 A.5.20, A.5.21

Only if: We use subcontractors to deliver our service = Yes

Every subcontractor with name, location and what they do for you. One per line is enough. Update it whenever you add or remove one.

We bind subcontractors to comparable security requirements

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(G) · ISO/IEC 27001:2022 A.5.20, A.5.21

Only if: We use subcontractors to deliver our service = Yes

Tick yes if your contracts with subcontractors contain security requirements that match what your customers ask of you, for example on incidents, access and data handling.

We inform customers of material changes, including where their data is processed

BOOLEAN · REQUIRED · LEGAL BASIS: ENISA TIG §5.1.4 · ISO/IEC 27001:2022 A.5.22

Tick yes if you tell customers before anything material changes in how you deliver: a takeover, a new subcontractor, another hosting provider, or a new country where their data is processed.

On request, we tell customers about security incidents that affected customers

BOOLEAN · REQUIRED · LEGAL BASIS: ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.22

Tick yes if, when a customer asks, you say openly whether and which security incidents affecting customers you had in the past.

We give customers the information their authority asks for

BOOLEAN · REQUIRED · LEGAL BASIS: ENISA TIG §5.1.4 · ISO/IEC 27001:2022 A.5.20, A.5.31

Tick yes if you give your customers the information their supervisory authority asks for after an incident or during an audit. Unless you are an essential or important entity under NIS 2 yourself, you owe that authority nothing directly; the duty is your customer's, and you help them meet it.

Everyone who works for our customers is bound to confidentiality

BOOLEAN · CONDITIONAL · LEGAL BASIS: ENISA TIG §5.1 TIPS; CIR 2024/2690 §10.3.2 · ISO/IEC 27001:2022 A.6.6

Only if: We process or store our customers' data = Yes or We access our customers' systems = Yes or Our staff enter our customers' premises = Yes

Tick yes if everyone who works for customers has signed a confidentiality commitment, in the employment contract or a separate agreement, or is bound by professional secrecy by law.

We check that staff who get access at customers are suitable

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §10.2.1 · ISO/IEC 27001:2022 A.6.1

Only if: We process or store our customers' data = Yes or We access our customers' systems = Yes or Our staff enter our customers' premises = Yes

Tick yes if, before they start, you check that people who will have access to customer data, systems or premises (key holders, for example) are suitable for that role, as far as employment and data protection law allow: references, for example, or a criminal record certificate where lawful and needed for the role. Checking every member of staff is not expected.

At contract end we hand back or destroy what we hold of the customer

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(H); §5.1.2(D) · ISO/IEC 27001:2022 A.5.11, A.8.10

Only if: We process or store our customers' data = Yes or We access our customers' systems = Yes or Our staff enter our customers' premises = Yes

Tick yes if your contract commits you to hand back the customer's data in a usable, documented format (for example CSV or JSON) and then delete it, return keys, badges and documents, and close accounts you had with them.

Data processing agreement (Art. 28 GDPR)

ENUM · CONDITIONAL · LEGAL BASIS: GDPR ART. 28(3); ART. 4(7) · ISO/IEC 27001:2022 A.5.34

Only if: We process or store our customers' data = Yes

Needed when you process personal data on a customer's behalf and on their instructions (Art. 28(3) GDPR). Some professions are controllers by law and sign none, in Germany tax advisers (§ 11(2) StBerG).

- ○ Yes, we offer a standard DPA
- ○ Not needed: we are an independent controller (for example a tax adviser)
- ○ Not needed: we process no personal data for customers
- ○ No

Customer data we hold electronically is encrypted

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(C); §9.2(A) · ISO/IEC 27001:2022 A.8.24

Only if: We process or store our customers' data = Yes

Tick yes if customer data is encrypted wherever you store it electronically: on servers, laptops, phones and backups, for example with BitLocker, FileVault or your cloud provider's disk encryption.

Customer data we send is encrypted in transit

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(C); §9.2(A) · ISO/IEC 27001:2022 A.8.24

Only if: We process or store our customers' data = Yes

Tick yes if your websites and interfaces use HTTPS with TLS 1.2 or higher, and files go to customers through an encrypted portal or encrypted email.

We run a documented information security management system (ISMS)

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(A) · ISO/IEC 27001:2022 A.5.1

Only if: We process or store our customers' data = Yes or We access our customers' systems = Yes or We provide SaaS / hosted services = Yes or We deliver on-prem software = Yes or We provide managed services / MSP = Yes

Tick yes if you have a written information security policy with assigned roles, regular reviews and documented incident handling. ISO/IEC 27001 certification, also on the basis of IT-Grundschutz, implies yes.

We hold a current security certificate or audit report that covers the service we deliver to customers

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(A); ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.19, A.5.22

Only if: We process or store our customers' data = Yes or We access our customers' systems = Yes or We provide SaaS / hosted services = Yes or We deliver on-prem software = Yes or We provide managed services / MSP = Yes

Counts: ISO/IEC 27001 (also on the basis of IT-Grundschutz), a BSI C5 attestation, a TISAX label, a SOC 2 Type II or ISAE 3402 report, or a European cybersecurity certificate. Tick yes only if its scope covers the service you deliver to customers.

Certificate or report: standard, issuer, valid until, scope

TEXT · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(A); ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.22

Only if: We hold a current security certificate or audit report that covers the service we deliver to customers = Yes

Copy the scope as it is printed on the certificate or report. Several? One per line.

We install security updates promptly and follow up known vulnerabilities

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(F) · ISO/IEC 27001:2022 A.8.8

Only if: We process or store our customers' data = Yes or We access our customers' systems = Yes or We provide SaaS / hosted services = Yes or We deliver on-prem software = Yes or We provide managed services / MSP = Yes

Tick yes if you have a set routine for security holes in the systems and software you use for customers: you learn about them, judge how urgent they are, and install the update or take another measure in time.

We have a written plan for security incidents

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(A); §3.1 · ISO/IEC 27001:2022 A.5.24, A.5.26

Only if: We process or store our customers' data = Yes or We access our customers' systems = Yes or We provide SaaS / hosted services = Yes or We deliver on-prem software = Yes or We provide managed services / MSP = Yes

Tick yes if a written plan sets out how you handle a security incident: who decides, who informs customers and who documents.

We have a written plan for outages, including backups

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(C); §4.1; §4.2 · ISO/IEC 27001:2022 A.5.29, A.5.30, A.8.13

Only if: We process or store our customers' data = Yes or We access our customers' systems = Yes or We provide SaaS / hosted services = Yes or We deliver on-prem software = Yes or We provide managed services / MSP = Yes

Tick yes if a written plan says how you keep working or restart after an outage, including backups of the data you hold for customers, kept apart from the live systems and test-restored. It names your critical systems, the fallback, and how long an outage may last and how much data may be lost at most.

All internal administrator accounts are protected with a second factor

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(A); §11.7 · ISO/IEC 27001:2022 A.8.5, A.8.2

Only if: We process or store our customers' data = Yes or We access our customers' systems = Yes or We provide SaaS / hosted services = Yes or We deliver on-prem software = Yes or We provide managed services / MSP = Yes

Tick yes if every account with administrator rights in your own systems (email, cloud, servers, accounting) needs a second factor to sign in, such as an authenticator app or a security key. Codes by SMS count but are the weakest option.

The systems we use to serve customers are security tested by an independent party

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(A); §6.5 · ISO/IEC 27001:2022 A.8.29, A.8.8

Only if: We provide SaaS / hosted services = Yes or We deliver on-prem software = Yes or We provide managed services / MSP = Yes

Tick yes if an independent party tests these systems for security holes, as often as your risk calls for. A penetration test and an external vulnerability scan both count.

We develop to defined secure development rules

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(A) · ISO/IEC 27001:2022 A.8.25, A.8.28

Only if: We provide SaaS / hosted services = Yes or We deliver on-prem software = Yes

Tick yes if your development follows set rules, for example a review before every change goes live, dependencies kept up to date, tests, and a check for known vulnerabilities. Asked only of suppliers who run software as a service or ship software.

We publish how to report a security hole to us

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(F); CRA ANNEX I PART II(5), (6) · ISO/IEC 27001:2022 A.8.8, A.5.21

Only if: We provide SaaS / hosted services = Yes or We deliver on-prem software = Yes

Tick yes if your website says how to report a security hole and what you then do, for example in a security.txt file (RFC 9116). From 11 December 2027 the Cyber Resilience Act requires such a policy and a contact address from makers of software products.

Access to customer systems uses personal accounts with a second factor

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(A); §11.3.2(A); §11.5.2(B) · ISO/IEC 27001:2022 A.8.2, A.8.5, A.5.16

Only if: We access our customers' systems = Yes

Tick yes if everyone who signs in to customer systems uses their own account with a second factor, including remote maintenance tools such as TeamViewer; nobody shares a login.

Administrative access to customer systems is logged

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(A); §3.2.3(E) · ISO/IEC 27001:2022 A.8.15

Only if: We access our customers' systems = Yes

Tick yes if it is recorded who accessed your customers' systems with administrator rights, and when, so it can be traced afterwards. Recording whole sessions is not expected.

We keep track of the keys, badges and codes customers give us

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(A); §11.2.2(D); §13.3.2(B) · ISO/IEC 27001:2022 A.7.2, A.5.11, A.5.18

Only if: Our staff enter our customers' premises = Yes

Tick yes if you always know who holds which key, badge or code, take it back when someone leaves or changes job, and tell the customer without delay when one is lost.

Our staff on customer premises follow written rules of conduct

BOOLEAN · CONDITIONAL · LEGAL BASIS: ENISA TIG §5.1 TIPS; CIR 2024/2690 §8.1.1 · ISO/IEC 27001:2022 A.7.2, A.7.7, A.6.3

Only if: Our staff enter our customers' premises = Yes

Tick yes if your staff have written rules for working at customers, for example: let no one in, leave screens, devices and documents alone, report anything unusual to the customer.

Customers' personal data outside the European Economic Area

ENUM · CONDITIONAL · LEGAL BASIS: GDPR ART. 44; ART. 45; ART. 46(2)(C); ART. 47

Only if: Data processing agreement (Art. 28 GDPR) = Yes, we offer a standard DPA or Data processing agreement (Art. 28 GDPR) = No

Whether you or your sub-processors transfer customers' personal data to a country outside the EEA, and on which basis. A transfer needs one of the bases of Chapter V GDPR (Art. 44).

- ○ No, it stays in the EEA
- ○ Yes, only to countries with an adequacy decision of the European Commission (Art. 45)
- ○ Yes, under the standard contractual clauses of the European Commission (Art. 46(2)(c))
- ○ Yes, under binding corporate rules (Art. 47)
- ○ Yes, on another basis

How you engage sub-processors

ENUM · CONDITIONAL · LEGAL BASIS: GDPR ART. 28(2)

Only if: Data processing agreement (Art. 28 GDPR) = Yes, we offer a standard DPA or Data processing agreement (Art. 28 GDPR) = No

A processor engages another processor only with the customer's prior specific or general written authorisation. Under a general one, it tells the customer of any intended addition or replacement, so the customer can object (Art. 28(2) GDPR).

- ○ General authorisation: we tell you before adding or replacing one, and you may object
- ○ We ask for your specific authorisation for each one
- ○ We engage no sub-processors for customers' personal data

We notify you of a personal data breach without undue delay after becoming aware of it

BOOLEAN · CONDITIONAL · LEGAL BASIS: GDPR ART. 33(2)

Only if: Data processing agreement (Art. 28 GDPR) = Yes, we offer a standard DPA or Data processing agreement (Art. 28 GDPR) = No

A processor owes this to the controller (Art. 33(2) GDPR). The controller needs it to meet its own duty to notify the supervisory authority (Art. 33(1)).

3. Software as a service (SaaS)

2 fields

Customers can protect their accounts with a second factor

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.2(C); §11.7 · ISO/IEC 27001:2022 A.8.5, A.5.23

Only if: We provide SaaS / hosted services = Yes

Tick yes if your application offers sign-in with a second factor (an authenticator app, a security key or a one-time code), at least for your customers' administrators. Your own internal admin accounts are a separate question under security practices.

Longest outage until your service is restored (hours)

INTEGER · CONDITIONAL · LEGAL BASIS: ENISA TIG §5.1 TIPS · ISO/IEC 27001:2022 A.5.30, A.5.23

Only if: We provide SaaS / hosted services = Yes

The most hours your service may be unavailable before it is restored. Give a value you keep.

4. Software on the customer's premises (on-premise)

4 fields

Until when you supply security updates for the version you deliver

STRING · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §6.1.2(B); CRA ART. 13(19) · ISO/IEC 27001:2022 A.5.21

Only if: We deliver on-prem software = Yes

Month and year, or the rule you apply. From 11 December 2027 the Cyber Resilience Act requires manufacturers to state this date at the time of purchase.

Deadline for security updates for critical vulnerabilities (hours)

INTEGER · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §5.1.4(F); CRA ANNEX I PART II(2) · ISO/IEC 27001:2022 A.8.8

Only if: We deliver on-prem software = Yes

Hours from a critical vulnerability becoming known to your fixed release. From 11 December 2027 the Cyber Resilience Act requires manufacturers to fix vulnerabilities without delay.

Customers can get a Software Bill of Materials (SBOM)

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §6.1.2(C); CRA ANNEX I PART II(1) · ISO/IEC 27001:2022 A.5.21

Only if: We deliver on-prem software = Yes

Tick yes if you give customers an SBOM for your releases (CycloneDX or SPDX). From 11 December 2027 the Cyber Resilience Act requires manufacturers to keep an SBOM in the technical documentation of products with digital elements; handing it to customers is up to you.

Releases and updates are signed

BOOLEAN · CONDITIONAL · LEGAL BASIS: CIR 2024/2690 §6.6.1(C); CRA ANNEX I PART II(7) · ISO/IEC 27001:2022 A.5.21

Only if: We deliver on-prem software = Yes

Tick yes if every release and update carries a signature your customers can check before installing, for example Sigstore, Authenticode or PGP.