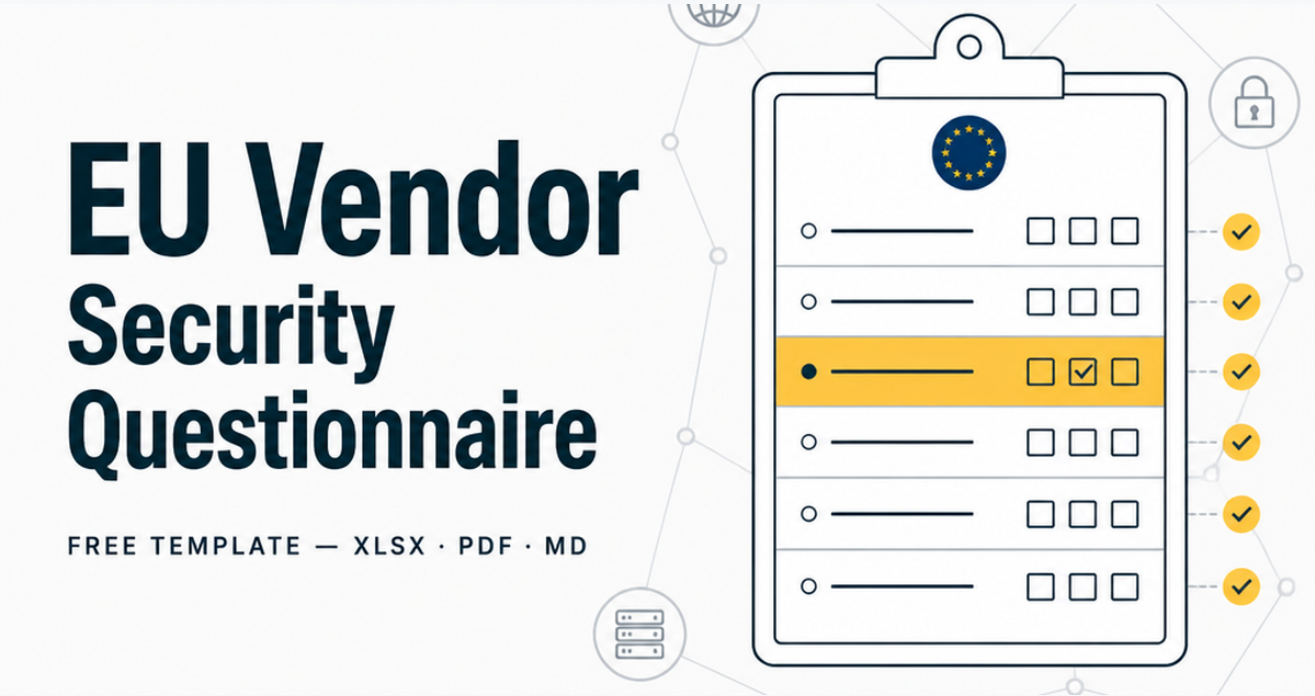

EU Vendor Security Questionnaire

67 questions in 10 sections, tiered by vendor criticality — the outbound question set for European buyers, covering what US-authored questionnaires don't ask: GDPR Article 28 processor terms, NIS2 supply-chain evidence, DORA provider fields, and data-residency / CLOUD Act exposure.

This PDF is the print/review companion. The working file is the XLSX (vendor register, tier rubric, filterable question bank with answer and reviewer dropdowns); a machine-readable Markdown variant ships for AI agents. All three are free at orbiqhq.com/templates/eu-vendor-security-questionnaire — no email required.

Legal anchors: GDPR Art 28 (Regulation (EU) 2016/679) · NIS2 Art 21(2)(d) (Directive (EU) 2022/2555) · DORA Art 28–30 (Regulation (EU) 2022/2554).

How to use the questionnaire

1. Tier the vendor. Score data sensitivity, system access, service criticality (including your own NIS2/DORA exposure) and substitutability 1–3 each. Total 10–12 → T1 (critical); 7–9 → T2 (standard); 4–6 → T3 (light).

2. Select the question subset. T3 vendors answer the 23 questions marked ALL; T2 vendors answer 46 (ALL + T1–T2); T1 vendors answer all 67, including the DORA addendum when you are a financial entity.

3. Demand evidence, not declarations. Every question names the artefact to attach — a certificate with scope, a pentest executive summary, a DPA clause. An answer without evidence is a self-declaration.

4. Assess and record. Mark each answer Adequate / Follow-up required / Deficient, log follow-ups, and record the overall outcome on the vendor register.

5. Re-run on cadence. T1 annually, T2 every 12–18 months, T3 every 2–3 years — with event triggers (incident, subcontractor change, certificate expiry) overriding the calendar.

Why an EU-native question set

The dominant standardized questionnaires are US-authored: SIG (licensed, ~850 questions in the Core scoped set) and CSA CAIQ v4 (free, 261 questions, cloud-focused). Neither asks the questions European buyers are now legally accountable for: whether the vendor's DPA carries all Article 28(3) clauses, whether an EU/EEA-only hosting option exists, whether a US parent exposes data to CLOUD Act or FISA 702 access, whether incident notification windows are compatible with NIS2 Article 23's 24-hour early warning, and whether the vendor can feed a DORA Register of Information. This questionnaire asks exactly those — alongside the security fundamentals every questionnaire needs.

Question bank (67 questions, 10 sections)

Tier column: ALL = every vendor · T1–T2 = standard and critical · T1 = critical only. Answer enum: Yes / Partial / No / N.A. — with evidence attached.

A — Company & Governance			
ID	**Question**	**Evidence requested**	**Tier**
A1	Do you have a named security leader (CISO or equivalent) and a dedicated security function?	Org chart extract or role description	ALL
A2	Do you maintain a documented, management-approved information security policy set, reviewed at least annually?	Policy index with last-review dates	ALL
A3	Do you hold a current ISO/IEC 27001:2022 certificate covering the service we buy?	Certificate with scope statement and expiry date	ALL
A4	Which other independent assurance do you hold (SOC 2 Type II, TISAX, C5, SecNumCloud)?	Report or certificate; bridge letter if report is older than 12 months	T1–T2
A5	Do you carry cyber liability insurance appropriate to the service?	Certificate of insurance (coverage amount, period)	T1–T2
A6	Are you in scope of NIS2 (essential/important entity) or DORA (financial entity / ICT third-party provider) yourself?	Statement of regulatory scope and registrations	T1–T2

B — GDPR & Data Protection (Article 28)			
ID	**Question**	**Evidence requested**	**Tier**
B1	Do you offer a Data Processing Agreement containing all Article 28(3) mandatory clauses?	DPA template (public link preferred)	ALL
B2	Do you process personal data only on documented instructions from the customer, including for international transfers?	DPA clause reference	ALL
B3	Are all persons authorised to process personal data bound by confidentiality commitments?	DPA clause reference or policy extract	T1–T2
B4	Do you maintain technical and organisational measures (TOMs) documentation aligned to GDPR Article 32?	TOMs annex or security whitepaper	ALL
B5	Do you publish a current subprocessor list, and do you operate a change-notice mechanism with an objection window?	Public subprocessor page URL + notice mechanism description	ALL
B6	Do you assist customers in fulfilling data subject rights requests (access, erasure, portability)?	DPA clause reference; feature or process description	T1–T2
B7	Do you commit to a personal data breach notification window that lets the customer meet its own 72-hour Article 33 duty?	Contractual notification clause with hours	ALL
B8	At contract end, do you delete or return all personal data (customer's choice) and delete existing copies?	DPA clause reference; deletion procedure	T1–T2
B9	Do you grant audit and information rights per Article 28(3)(h), including third-party audits mandated by the customer?	DPA clause reference	T1
B10	Have you appointed a Data Protection Officer or EU representative (Article 27) where required?	DPO/representative contact details	T1–T2

C — Data Residency & Sovereignty			
ID	**Question**	**Evidence requested**	**Tier**
C1	In which countries/regions are production data and backups stored and processed?	Data-location statement per environment	ALL
C2	Do you offer an EU/EEA-only hosting option for both data at rest and processing (including support access)?	Region/deployment documentation	ALL
C3	Which transfer mechanism covers any third-country transfers (adequacy decision, SCCs, EU-US DPF)?	Transfer-mechanism inventory; SCC module references	T1–T2
C4	Is your corporate structure subject to non-EU jurisdiction (e.g. US parent) that could compel disclosure under the US CLOUD Act?	Corporate-structure statement; policy for handling government requests	T1–T2

C — Data Residency & Sovereignty			
ID	**Question**	**Evidence requested**	**Tier**
C5	Have you performed a transfer impact assessment addressing FISA Section 702-type access, and can you share it?	TIA summary or Schrems II analysis	T1
C6	Is customer data encrypted in transit (TLS 1.2+) and at rest (AES-256 or equivalent)?	Encryption standards documentation	ALL
C7	Can encryption keys be held or controlled by the customer or an EU-only entity (BYOK/HYOK)?	Key-management architecture description	T1
C8	Do you publish a transparency report or policy for responding to government data requests?	Transparency report URL or policy	T1

D — Access Control & Identity			
ID	**Question**	**Evidence requested**	**Tier**
D1	Is multi-factor authentication enforced for all staff access to production and customer data?	IAM policy extract; MFA coverage statement	ALL
D2	Do you support SSO (SAML/OIDC) and SCIM provisioning for customer tenants?	Product security documentation	T1–T2
D3	Is access to customer data role-based and least-privilege, with production access restricted to a named group?	Access-control policy; role matrix	ALL
D4	Are user access rights reviewed on a defined cadence (at least quarterly for privileged access)?	Most recent access-review record (redacted)	T1–T2
D5	Are privileged accounts managed through a PAM solution with session logging?	PAM tooling description	T1
D6	Does your joiner/mover/leaver process revoke access within a defined SLA on termination?	Process description with SLA	T1–T2
D7	Do you perform background screening of employees with access to customer data, where lawful?	Screening policy statement	T1

E — Infrastructure & Operations			
ID	**Question**	**Evidence requested**	**Tier**
E1	Describe your hosting model (cloud provider(s), regions, single/multi-tenant).	Architecture overview	ALL
E2	Are production, staging and development environments segregated, with no customer data in non-production?	Environment policy; data-masking approach	T1–T2
E3	Do you operate a vulnerability management programme with defined remediation SLAs for critical findings?	Policy + time-to-patch metrics for the last 6-12 months	ALL
E4	Is the service penetration-tested at least annually by an independent party, and will you share the executive summary?	Latest pentest executive summary with remediation status	ALL
E5	Are endpoints protected with EDR/anti-malware, and are servers hardened to a documented baseline?	Tooling and baseline description	T1–T2
E6	Do you centrally log security events and monitor them (SIEM/SOC), with defined retention?	Logging/monitoring description; retention period	T1–T2
E7	Is infrastructure configuration managed as code / under change control with peer review?	Change-management process description	T1
E8	Do you have DDoS protection and capacity management for availability-critical components?	Provider/technology statement	T1

F — Incident Management & Notification			
ID	**Question**	**Evidence requested**	**Tier**
F1	Do you maintain a tested incident response plan with defined roles and severity levels?	IR plan summary; date of last test/exercise	ALL

F — Incident Management & Notification			
ID	**Question**	**Evidence requested**	**Tier**
F2	Do you provide a 24/7 security incident contact for customers?	Contact details / escalation path	ALL
F3	What is your contractual window for notifying customers of incidents affecting their service or data (in hours)?	Contract clause; must be compatible with the customer's NIS2 Article 23 24-hour early-warning duty	ALL
F4	For financial-entity customers: can you support their DORA major-incident reporting timelines with timely information?	Process description referencing DORA Article 19	T1
F5	Can you preserve and share forensic evidence related to incidents affecting the customer?	Evidence-handling procedure	T1
F6	Do you provide post-incident reports (root cause, impact, corrective actions) to affected customers?	Sample or template post-incident report	T1–T2

G — Business Continuity & Disaster Recovery			
ID	**Question**	**Evidence requested**	**Tier**
G1	Do you maintain business continuity and disaster recovery plans covering the service we buy?	BCP/DR plan extract	ALL
G2	What are your committed RTO and RPO for the service?	SLA or DR documentation	T1–T2
G3	Are backups encrypted, geographically separated, and restore-tested on a defined cadence?	Backup policy; last restore-test date and result	ALL
G4	When did you last test your DR plan, and what were the results?	DR test report summary	T1
G5	Which critical dependencies (providers, regions, single points of failure) does the service have?	Dependency/concentration statement	T1

H — Secure Development			
ID	**Question**	**Evidence requested**	**Tier**
H1	Do you follow a documented secure development lifecycle with security requirements per release?	SDLC policy summary	T1–T2
H2	Is code peer-reviewed and scanned (SAST/DAST/dependency scanning) before production deployment?	CI/CD security-gate description	T1–T2
H3	Do you maintain an SBOM or dependency inventory for the service, and monitor it for vulnerabilities?	SBOM availability statement (format, cadence)	T1
H4	Are secrets and credentials managed in a dedicated vault (never in code repositories)?	Secrets-management description	T1–T2
H5	Do developers receive secure-coding training on a defined cadence?	Training programme statement	T1
H6	Is security testing performed on major releases and architectural changes?	Release security-testing process	T1

I — Subcontractors & Supply Chain			
ID	**Question**	**Evidence requested**	**Tier**
I1	Do you maintain a current register of subcontractors involved in delivering the service, with locations and roles?	Subcontractor register	ALL
I2	Do your subcontractor contracts flow down equivalent security and data protection obligations?	Flow-down clause statement	T1–T2
I3	Do you assess your own suppliers' security before onboarding and on a defined cadence?	Supplier assessment process description	T1–T2
I4	Will you notify us of subcontractor changes in advance, with a right to object?	Contract clause; notice window	ALL
I5	Do you support customer exit: data export in an open format, migration assistance, and a defined exit plan?	Exit/portability documentation (cf. DORA Article 28(8) for financial entities)	T1–T2

I — Subcontractors & Supply Chain			
ID	**Question**	**Evidence requested**	**Tier**
I6	Can you pass through supplier evidence requested under our NIS2 Article 21(2)(d) supply-chain duties?	Commitment statement; evidence-sharing process	T1

J — Financial-Entity Addendum (DORA)			
ID	**Question**	**Evidence requested**	**Tier**
J1	Can you provide the data fields financial-entity customers need for their DORA Register of Information (LEI, service type, data locations)?	RoI field sheet (cf. ITS (EU) 2024/2956)	T1
J2	Do your contracts for critical/important functions include the DORA Article 30(3) provisions (access, audit, termination, exit)?	Contract template references	T1
J3	Are you aware of, or preparing for, designation as a critical ICT third-party provider under DORA oversight?	Statement	T1
J4	Will you participate in the customer's threat-led penetration testing (TLPT) where required?	Commitment statement (cf. DORA Articles 26-27)	T1
J5	Do you support documented exit strategies including transition assistance and parallel-run periods?	Exit-strategy documentation	T1

From questionnaire to continuous assurance

A questionnaire is a snapshot; vendor risk is a stream. Orbiq's vendor assurance platform runs the same tiering, question sets, evidence collection and review workflow continuously — with AI-evaluated responses and an audit trail generated as a by-product. See orbiqhq.com/platform/vendor-assurance-platform.

Version 1.0 · published 2026-07-13 · Free to use; attribution appreciated. Source: orbiqhq.com/templates/eu-vendor-security-questionnaire