EU-beveiligingsvragenlijst voor leveranciers

67 vragen in 10 secties, ingedeeld naar de criticaliteit van de leverancier — de uitgaande vragenset voor Europese afnemers, die behandelt wat Amerikaanse vragenlijsten niet vragen: verwerkersbepalingen uit artikel 28 AVG, ketenbewijs onder NIS2, velden voor DORA-leveranciers en blootstelling via gegevenslocatie en de CLOUD Act.

Dit PDF is de print- en reviewmetgezel. Het werkbestand is de XLSX (leveranciersregister, niveaurubriek, filterbare vragenbank met keuzelijsten voor antwoord en beoordeling); een machine-leesbare Markdown-variant is er voor AI-agents. Alle drie zijn gratis op orbiqhq.com/templates/eu-vendor-security-questionnaire — geen e-mail vereist.

Juridische grondslagen: artikel 28 AVG (Verordening (EU) 2016/679) · artikel 21, lid 2, onder d), NIS2 (Richtlijn (EU) 2022/2555) · artikel 28–30 DORA (Verordening (EU) 2022/2554). Dit sjabloon is een hulpmiddel, geen juridisch advies.

Zo gebruikt u de vragenlijst

1. Bepaal het niveau van de leverancier. Scoor de gevoeligheid van gegevens, de systeemtoegang, de criticaliteit van de dienst (inclusief uw eigen blootstelling aan NIS2/DORA) en de vervangbaarheid elk 1–3. Totaal 10–12 → T1 (kritiek); 7–9 → T2 (standaard); 4–6 → T3 (licht).

2. Selecteer de vragenset. T3-leveranciers beantwoorden de 23 vragen met de markering ALLE; T2-leveranciers beantwoorden er 46 (ALLE + T1–T2); T1-leveranciers beantwoorden alle 67, inclusief het DORA-addendum wanneer u een financiële entiteit bent.

3. Vraag om bewijs, niet om verklaringen. Bij elke vraag staat welk artefact moet worden bijgevoegd — een certificaat met scope, een managementsamenvatting van een pentest, een bepaling uit de verwerkersovereenkomst. Een antwoord zonder bewijs is een eigen verklaring.

4. Beoordeel en leg vast. Markeer elk antwoord als Toereikend / Opvolging vereist / Ontoereikend, leg de opvolging vast en noteer de eindconclusie in het leveranciersregister.

5. Herhaal op frequentie. T1 jaarlijks, T2 elke 12–18 maanden, T3 elke 2–3 jaar — waarbij triggers op gebeurtenissen (incident, wisseling van onderaannemer, verlopen certificaat) vóór de kalender gaan.

Waarom een Europese vragenset

De dominante gestandaardiseerde vragenlijsten zijn van Amerikaanse makelij: SIG (gelicentieerd, ~850 vragen in de Core-set) en CSA CAIQ v4 (gratis, 261 vragen, cloudgericht). Geen van beide stelt de vragen waarvoor Europese afnemers inmiddels juridisch verantwoordelijk zijn: of de verwerkersovereenkomst van de leverancier alle bepalingen van artikel 28, lid 3, bevat, of er een hostingoptie uitsluitend binnen de EU/EER bestaat, of een Amerikaanse moeder gegevens blootstelt aan toegang onder de CLOUD Act of FISA 702, of de meldtermijnen voor incidenten verenigbaar zijn met de vroegtijdige waarschuwing binnen 24 uur uit artikel 23 NIS2, en of de leverancier een DORA-informatieregister kan voeden. Deze vragenlijst stelt precies die vragen — naast de beveiligingsbasics die in elke vragenlijst thuishoren.

Vragenbank (67 vragen, 10 secties)

Kolom Niveau: ALLE = elke leverancier · T1–T2 = standaard en kritiek · T1 = alleen kritiek. Antwoordenum: Ja / Gedeeltelijk / Nee / N.v.t. — met bewijs bijgevoegd.

A — Bedrijf & governance

ID	Vraag	Gevraagd bewijs	Niveau
A1	Heeft u een bij naam genoemde security-verantwoordelijke (CISO of gelijkwaardig) en een specifieke securityfunctie?	Uittreksel organogram of functieomschrijving	ALLE
A2	Onderhoudt u een gedocumenteerde, door het management goedgekeurde set informatiebeveiligingsbeleid, dat ten minste jaarlijks wordt herzien?	Beleidsindex met datums van de laatste herziening	ALLE
A3	Beschikt u over een geldig ISO/IEC 27001:2022-certificaat dat de dienst dekt die wij afnemen?	Certificaat met scopeverklaring en vervaldatum	ALLE
A4	Over welke andere onafhankelijke assurance beschikt u (SOC 2 Type II, TISAX, C5, SecNumCloud)?	Rapport of certificaat; bridge letter als het rapport ouder is dan 12 maanden	T1–T2
A5	Heeft u een cyberaansprakelijkheidsverzekering die passend is bij de dienst?	Verzekeringsbewijs (dekkingsbedrag, looptijd)	T1–T2
A6	Valt u zelf onder NIS2 (essentiële/belangrijke entiteit) of DORA (financiële entiteit / ICT-derde-aanbieder)?	Verklaring over de toezichtsreikwijdte en registraties	T1–T2

B — AVG & gegevensbescherming (artikel 28)

ID	Vraag	Gevraagd bewijs	Niveau
B1	Biedt u een verwerkersovereenkomst aan die alle verplichte bepalingen van artikel 28, lid 3, bevat?	Sjabloon verwerkersovereenkomst (bij voorkeur een openbare link)	ALLE
B2	Verwerkt u persoonsgegevens uitsluitend op gedocumenteerde instructie van de klant, ook bij internationale doorgiften?	Verwijzing naar de bepaling in de verwerkersovereenkomst	ALLE
B3	Zijn alle personen die gemachtigd zijn persoonsgegevens te verwerken gebonden aan geheimhouding?	Verwijzing naar de bepaling in de verwerkersovereenkomst of uittreksel uit het beleid	T1–T2
B4	Onderhoudt u documentatie over technische en organisatorische maatregelen (TOM's) die aansluit op artikel 32 AVG?	TOM-bijlage of security-whitepaper	ALLE
B5	Publiceert u een actuele lijst van subverwerkers, en hanteert u een mechanisme voor wijzigingsmeldingen met een bezwaartermijn?	URL van de openbare subverwerkerspagina + beschrijving van het meldmechanisme	ALLE
B6	Ondersteunt u klanten bij het afhandelen van verzoeken van betrokkenen (inzage, wissing, overdraagbaarheid)?	Verwijzing naar de bepaling in de verwerkersovereenkomst; beschrijving van de functionaliteit of het proces	T1–T2
B7	Zegt u een meldtermijn voor datalekken toe waarmee de klant zijn eigen 72-uursplicht uit artikel 33 kan nakomen?	Contractuele meldbepaling met het aantal uren	ALLE
B8	Wist of retourneert u aan het einde van het contract alle persoonsgegevens (naar keuze van de klant) en wist u bestaande kopieën?	Verwijzing naar de bepaling in de verwerkersovereenkomst; wisprocedure	T1–T2
B9	Verleent u audit- en informatierechten conform artikel 28, lid 3, onder h), inclusief door de klant aangewezen externe audits?	Verwijzing naar de bepaling in de verwerkersovereenkomst	T1

ID	Vraag	Gevraagd bewijs	Niveau
B10	Heeft u waar vereist een functionaris voor gegevensbescherming of een EU-vertegenwoordiger (artikel 27) aangesteld?	Contactgegevens van de FG/vertegenwoordiger	T1–T2

C — Gegevenslocatie & soevereiniteit

ID	Vraag	Gevraagd bewijs	Niveau
C1	In welke landen/regio's worden productiegegevens en back-ups opgeslagen en verwerkt?	Verklaring over gegevenslocaties per omgeving	ALLE
C2	Biedt u een hostingoptie uitsluitend binnen de EU/EER, zowel voor gegevens in rust als voor verwerking (inclusief supporttoegang)?	Documentatie over regio's/uitrol	ALLE
C3	Welk doorgiftemechanisme dekt eventuele doorgiften naar derde landen (adequaatheidsbesluit, SCC's, EU-US DPF)?	Overzicht van doorgiftemechanismen; verwijzingen naar de SCC-modules	T1–T2
C4	Valt uw ondernemingsstructuur onder een jurisdictie buiten de EU (bijv. een Amerikaanse moeder) die verstrekking op grond van de Amerikaanse CLOUD Act kan afdwingen?	Verklaring over de ondernemingsstructuur; beleid voor de afhandeling van overheidsverzoeken	T1–T2
C5	Heeft u een transfer impact assessment uitgevoerd dat ingaat op toegang van het type FISA Section 702, en kunt u die delen?	Samenvatting van de TIA of Schrems II-analyse	T1
C6	Worden klantgegevens versleuteld tijdens transport (TLS 1.2+) en in rust (AES-256 of gelijkwaardig)?	Documentatie over versleutelingsstandaarden	ALLE
C7	Kunnen de versleutelingssleutels worden beheerd of gecontroleerd door de klant of door een entiteit uitsluitend binnen de EU (BYOK/HYOK)?	Beschrijving van de architectuur voor sleutelbeheer	T1
C8	Publiceert u een transparantierapport of beleid voor de afhandeling van gegevensverzoeken van overheden?	URL van het transparantierapport of het beleid	T1

D — Toegangsbeheer & identiteit

ID	Vraag	Gevraagd bewijs	Niveau
D1	Is multifactorauthenticatie afgedwongen voor alle medewerkerstoegang tot productie en klantgegevens?	Uittreksel IAM-beleid; verklaring over de MFA-dekking	ALLE
D2	Ondersteunt u SSO (SAML/OIDC) en SCIM-provisioning voor klanttenants?	Documentatie over productbeveiliging	T1–T2
D3	Is de toegang tot klantgegevens rolgebaseerd en volgens het principe van minimale rechten, met productietoegang beperkt tot een benoemde groep?	Toegangsbeleid; rollenmatrix	ALLE
D4	Worden toegangsrechten van gebruikers op een vastgestelde frequentie beoordeeld (ten minste per kwartaal bij geprivilegieerde toegang)?	Meest recente vastlegging van de toegangsreview (geanonimiseerd)	T1–T2
D5	Worden geprivilegieerde accounts beheerd via een PAM-oplossing met sessielogging?	Beschrijving van de PAM-tooling	T1
D6	Trekt uw instroom-/doorstroom-/uitstroomproces de toegang bij beëindiging binnen een vastgestelde SLA in?	Procesbeschrijving met SLA	T1–T2
D7	Voert u, waar wettelijk toegestaan, een achtergrondscreening uit bij medewerkers met toegang tot klantgegevens?	Verklaring over het screeningbeleid	T1

E — Infrastructuur & operations

ID	Vraag	Gevraagd bewijs	Niveau
E1	Beschrijf uw hostingmodel (cloudleverancier(s), regio's, single- of multitenant).	Architectuuroverzicht	ALLE
E2	Zijn de productie-, staging- en ontwikkelomgevingen gescheiden, zonder klantgegevens buiten productie?	Omgevingsbeleid; aanpak voor het maskeren van gegevens	T1–T2
E3	Voert u een programma voor kwetsbaarhedenbeheer met vastgestelde hersteltermijnen (SLA's) voor kritieke bevindingen?	Beleid + time-to-patch-cijfers over de afgelopen 6-12 maanden	ALLE
E4	Wordt de dienst ten minste jaarlijks door een onafhankelijke partij aan een penetratietest onderworpen, en deelt u de managementsamenvatting?	Managementsamenvatting van de laatste pentest met de herstelstatus	ALLE
E5	Zijn endpoints beschermd met EDR/antimalware, en zijn servers gehard volgens een gedocumenteerde basislijn?	Beschrijving van de tooling en de basislijn	T1–T2
E6	Logt u beveiligingsgebeurtenissen centraal en monitort u die (SIEM/SOC), met een vastgestelde bewaartermijn?	Beschrijving van logging/monitoring; bewaartermijn	T1–T2
E7	Wordt de infrastructuurconfiguratie als code beheerd / onder wijzigingsbeheer met collegiale toetsing?	Beschrijving van het wijzigingsbeheerproces	T1
E8	Beschikt u over DDoS-bescherming en capaciteitsbeheer voor componenten die kritiek zijn voor de beschikbaarheid?	Verklaring over de leverancier/technologie	T1

F — Incidentbeheer & melding

ID	Vraag	Gevraagd bewijs	Niveau
F1	Onderhoudt u een getest incidentresponsplan met vastgestelde rollen en ernstniveaus?	Samenvatting van het IR-plan; datum van de laatste test/oefening	ALLE
F2	Biedt u klanten een 24/7-contactpunt voor beveiligingsincidenten?	Contactgegevens / escalatiepad	ALLE
F3	Wat is uw contractuele termijn (in uren) om klanten te informeren over incidenten die hun dienst of gegevens raken?	Contractbepaling; moet verenigbaar zijn met de 24-uursplicht tot vroegtijdige waarschuwing van de klant uit artikel 23 NIS2	ALLE
F4	Voor klanten die financiële entiteit zijn: kunt u hun meldtermijnen voor ernstige incidenten onder DORA ondersteunen met tijdige informatie?	Procesbeschrijving met verwijzing naar artikel 19 DORA	T1
F5	Kunt u forensisch bewijs met betrekking tot incidenten die de klant raken veiligstellen en delen?	Procedure voor de omgang met bewijs	T1
F6	Verstrekt u getroffen klanten evaluatierapporten na incidenten (onderliggende oorzaak, impact, corrigerende maatregelen)?	Voorbeeld of sjabloon van een evaluatierapport na een incident	T1–T2

G — Bedrijfscontinuïteit & uitwijk

ID	Vraag	Gevraagd bewijs	Niveau
G1	Onderhoudt u bedrijfscontinuïteits- en uitwijkplannen die de dienst dekken die wij afnemen?	Uittreksel uit het BCP-/uitwijkplan	ALLE
G2	Welke RTO en RPO zegt u voor de dienst toe?	SLA- of uitwijkdocumentatie	T1–T2
G3	Zijn back-ups versleuteld, geografisch gescheiden en op een vastgestelde frequentie getest op herstel?	Back-upbeleid; datum en uitkomst van de laatste hersteltest	ALLE
G4	Wanneer heeft u uw uitwijkplan voor het laatst getest, en wat waren de resultaten?	Samenvatting van het testrapport van de uitwijk	T1

ID	Vraag	Gevraagd bewijs	Niveau
G5	Welke kritieke afhankelijkheden (leveranciers, regio's, single points of failure) kent de dienst?	Verklaring over afhankelijkheden/concentratie	T1

H — Veilige ontwikkeling

ID	Vraag	Gevraagd bewijs	Niveau
H1	Volgt u een gedocumenteerde secure development lifecycle met beveiligingseisen per release?	Samenvatting van het SDLC-beleid	T1–T2
H2	Wordt code collegiaal getoetst en gescand (SAST/DAST/dependency scanning) vóór uitrol naar productie?	Beschrijving van de security gates in CI/CD	T1–T2
H3	Onderhoudt u een SBOM of een overzicht van afhankelijkheden voor de dienst, en monitort u die op kwetsbaarheden?	Verklaring over de beschikbaarheid van de SBOM (formaat, frequentie)	T1
H4	Worden secrets en inloggegevens beheerd in een daarvoor bestemde vault (nooit in coderepository's)?	Beschrijving van het beheer van secrets	T1–T2
H5	Krijgen ontwikkelaars op een vastgestelde frequentie training in veilig programmeren?	Verklaring over het opleidingsprogramma	T1
H6	Worden grote releases en architectuurwijzigingen aan beveiligingstesten onderworpen?	Proces voor beveiligingstesten bij releases	T1

I — Onderaannemers & toeleveringsketen

ID	Vraag	Gevraagd bewijs	Niveau
I1	Onderhoudt u een actueel register van onderaannemers die bij de dienstverlening betrokken zijn, met locaties en rollen?	Register van onderaannemers	ALLE
I2	Leggen uw contracten met onderaannemers gelijkwaardige verplichtingen op het gebied van beveiliging en gegevensbescherming door?	Verklaring over de doorlegbepaling	T1–T2
I3	Beoordeelt u de beveiliging van uw eigen leveranciers vóór onboarding en op een vastgestelde frequentie?	Beschrijving van het beoordelingsproces voor leveranciers	T1–T2
I4	Informeert u ons vooraf over wijzigingen bij onderaannemers, met een recht van bezwaar?	Contractbepaling; meldtermijn	ALLE
I5	Ondersteunt u de exit van klanten: gegevensexport in een open formaat, migratiehulp en een vastgesteld exitplan?	Documentatie over exit/overdraagbaarheid (vgl. artikel 28, lid 8, DORA voor financiële entiteiten)	T1–T2
I6	Kunt u leveranciersbewijs doorgeven dat wij opvragen op grond van onze ketenverplichtingen uit artikel 21, lid 2, onder d), NIS2?	Verklaring van toezegging; proces voor het delen van bewijs	T1

J — Addendum voor financiële entiteiten (DORA)

ID	Vraag	Gevraagd bewijs	Niveau
J1	Kunt u de gegevensvelden leveren die klanten die financiële entiteit zijn nodig hebben voor hun DORA-informatieregister (LEI, type dienst, gegevenslocaties)?	Veldenblad voor het informatieregister (vgl. ITS (EU) 2024/2956)	T1
J2	Bevatten uw contracten voor kritieke/belangrijke functies de bepalingen van artikel 30, lid 3, DORA (toegang, audit, beëindiging, exit)?	Verwijzingen naar de contractsjablonen	T1

ID	Vraag	Gevraagd bewijs	Niveau
J3	Bent u bekend met, of bereidt u zich voor op, aanwijzing als kritieke ICT-derde-aanbieder onder DORA-toezicht?	Verklaring	T1
J4	Neemt u waar vereist deel aan de dreigingsgestuurde penetratietesten (TLPT) van de klant?	Verklaring van toezegging (vgl. artikel 26-27 DORA)	T1
J5	Ondersteunt u gedocumenteerde exitstrategieën, inclusief transitiehulp en perioden van parallelle uitvoering?	Documentatie over de exitstrategie	T1

Van vragenlijst naar continue assurance

Een vragenlijst is een momentopname; leveranciersrisico is een stroom. Het vendor assurance-platform van Orbiq draait dezelfde indeling in niveaus, vragensets, bewijsverzameling en reviewworkflow doorlopend — met door AI beoordeelde reacties en een audittrail die als bijproduct ontstaat. Zie orbiqhq.com/platform/vendor-assurance-platform.

Versie 1.0 · gepubliceerd 2026-07-13 · Vrij te gebruiken; bronvermelding gewaardeerd. Bron: orbiqhq.com/templates/eu-vendor-security-questionnaire