Questionnaire de sécurité fournisseurs UE

67 questions en 10 sections, graduées selon la criticité du fournisseur — le jeu de questions sortant des acheteurs européens, qui couvre ce que les questionnaires d'origine américaine ne demandent pas : clauses sous-traitant de l'article 28 du RGPD, preuves de sécurité de la chaîne d'approvisionnement NIS2, champs prestataires DORA, et exposition à la localisation des données et au CLOUD Act.

Ce PDF est le compagnon d'impression et de revue. Le fichier de travail est le XLSX (registre des fournisseurs, grille de niveaux, banque de questions filtrable avec listes déroulantes de réponse et d'évaluation) ; une variante Markdown lisible par machine est fournie pour les agents IA. Les trois fichiers sont gratuits sur orbiqhq.com/templates/eu-vendor-security-questionnaire — sans e-mail requis.

Ancrages juridiques : art. 28 du RGPD (règlement (UE) 2016/679) · art. 21(2)(d) de NIS2 (directive (UE) 2022/2555) · art. 28 à 30 de DORA (règlement (UE) 2022/2554).

Comment utiliser le questionnaire

1. Classez le fournisseur par niveau. Notez de 1 à 3 la sensibilité des données, l'accès aux systèmes, la criticité du service (y compris votre propre exposition NIS2/DORA) et la substituabilité. Total de 10-12 → T1 (critique) ; 7-9 → T2 (standard) ; 4-6 → T3 (allégé).

2. Sélectionnez le sous-ensemble de questions. Les fournisseurs T3 répondent aux 23 questions marquées TOUS ; les fournisseurs T2 en traitent 46 (TOUS + T1-T2) ; les fournisseurs T1 répondent aux 67 questions, y compris l'addendum DORA lorsque vous êtes une entité financière.

3. Exigez des preuves, pas des déclarations. Chaque question nomme le document à joindre — un certificat avec son périmètre, une synthèse de test d'intrusion, une clause de DPA. Une réponse sans preuve est une déclaration sur l'honneur.

4. Évaluez et consignez. Marquez chaque réponse Adéquat / Suivi requis / Insuffisant, consignez les actions de suivi et enregistrez le résultat global dans le registre des fournisseurs.

5. Relancez selon la périodicité définie. T1 chaque année, T2 tous les 12 à 18 mois, T3 tous les 2 à 3 ans — les déclencheurs événementiels (incident, changement de sous-traitant, expiration d'un certificat) primant sur le calendrier.

Pourquoi un jeu de questions pensé pour l'UE

Les questionnaires standardisés dominants sont d'origine américaine : SIG (sous licence, ~850 questions dans le périmètre Core) et CSA CAIQ v4 (gratuit, 261 questions, centré sur le cloud). Ni l'un ni l'autre ne pose les questions dont les acheteurs européens sont désormais juridiquement comptables : le DPA du fournisseur comporte-t-il toutes les clauses de l'article 28(3), existe-t-il une option d'hébergement exclusivement UE/EEE, une société mère américaine expose-t-elle les données à un accès au titre du CLOUD Act ou de la section 702 du FISA, les délais de notification d'incident sont-ils compatibles avec l'alerte précoce à 24 heures de l'article 23 de NIS2, et le fournisseur peut-il alimenter un registre d'informations DORA ? Ce questionnaire pose exactement ces questions — aux côtés des fondamentaux de sécurité que tout questionnaire doit couvrir.

Banque de questions (67 questions, 10 sections)

Colonne Niveau : TOUS = tous les fournisseurs · T1-T2 = standard et critique · T1 = critique uniquement. Énumération des réponses : Oui / Partiel / Non / N.A. — preuve à l'appui.

A — Entreprise et gouvernance

ID	Question	Preuves demandées	Niveau
A1	Disposez-vous d'un responsable sécurité désigné (RSSI ou équivalent) et d'une fonction sécurité dédiée ?	Extrait d'organigramme ou description de poste	TOUS
A2	Maintenez-vous un corpus documenté de politiques de sécurité de l'information, approuvé par la direction et revu au moins une fois par an ?	Index des politiques avec dates de dernière revue	TOUS
A3	Détenez-vous un certificat ISO/IEC 27001:2022 en cours de validité couvrant le service que nous achetons ?	Certificat avec énoncé du périmètre et date d'expiration	TOUS
A4	Quelles autres attestations indépendantes détenez-vous (SOC 2 Type II, TISAX, C5, SecNumCloud) ?	Rapport ou certificat ; lettre de liaison (bridge letter) si le rapport date de plus de 12 mois	T1-T2
A5	Disposez-vous d'une assurance cyber adaptée au service ?	Attestation d'assurance (montant de la couverture, période)	T1-T2
A6	Êtes-vous vous-même dans le champ de NIS2 (entité essentielle/importante) ou de DORA (entité financière / prestataire tiers de services TIC) ?	Déclaration du périmètre réglementaire et des enregistrements	T1-T2

B — RGPD et protection des données (article 28)

ID	Question	Preuves demandées	Niveau
B1	Proposez-vous un accord de traitement des données (DPA) contenant toutes les clauses obligatoires de l'article 28(3) ?	Modèle de DPA (lien public de préférence)	TOUS
B2	Traitez-vous les données personnelles uniquement sur instruction documentée du client, y compris pour les transferts internationaux ?	Référence de la clause du DPA	TOUS
B3	Toutes les personnes autorisées à traiter des données personnelles sont-elles soumises à des engagements de confidentialité ?	Référence de la clause du DPA ou extrait de politique	T1-T2
B4	Maintenez-vous une documentation des mesures techniques et organisationnelles (TOM) alignée sur l'article 32 du RGPD ?	Annexe TOM ou livre blanc sécurité	TOUS
B5	Publiez-vous une liste à jour de vos sous-traitants ultérieurs, avec un mécanisme de notification des changements assorti d'une fenêtre d'objection ?	URL de la page publique des sous-traitants ultérieurs + description du mécanisme de notification	TOUS
B6	Assistez-vous vos clients dans le traitement des demandes d'exercice des droits des personnes concernées (accès, effacement, portabilité) ?	Référence de la clause du DPA ; description de la fonctionnalité ou du processus	T1-T2
B7	Vous engagez-vous sur un délai de notification des violations de données personnelles permettant au client de respecter sa propre obligation de 72 heures (article 33) ?	Clause contractuelle de notification avec délai en heures	TOUS
B8	À la fin du contrat, supprimez-vous ou restituez-vous l'ensemble des données personnelles (au choix du client), en supprimant les copies existantes ?	Référence de la clause du DPA ; procédure de suppression	T1-T2
B9	Accordez-vous des droits d'audit et d'information conformes à l'article 28(3)(h), y compris des audits par des tiers mandatés par le client ?	Référence de la clause du DPA	T1
B10	Avez-vous désigné un délégué à la protection des données (DPO) ou un représentant dans l'UE (article 27) lorsque c'est requis ?	Coordonnées du DPO/représentant	T1-T2

C — Localisation et souveraineté des données

ID	Question	Preuves demandées	Niveau
C1	Dans quels pays/régions les données de production et les sauvegardes sont-elles stockées et traitées ?	Déclaration de localisation des données par environnement	TOUS
C2	Proposez-vous une option d'hébergement exclusivement UE/EEE, couvrant le stockage comme le traitement (y compris l'accès du support) ?	Documentation des régions/déploiements	TOUS
C3	Quel mécanisme couvre les éventuels transferts vers un pays tiers (décision d'adéquation, CCT, EU-US DPF) ?	Inventaire des mécanismes de transfert ; références des modules CCT	T1-T2
C4	Votre structure de groupe relève-t-elle d'une juridiction hors UE (p. ex. maison mère américaine) susceptible de contraindre à une divulgation au titre du CLOUD Act américain ?	Déclaration sur la structure du groupe ; politique de traitement des demandes gouvernementales	T1-T2
C5	Avez-vous réalisé une analyse d'impact des transferts (TIA) traitant les accès de type FISA 702, et pouvez-vous la partager ?	Synthèse de la TIA ou analyse Schrems II	T1
C6	Les données client sont-elles chiffrées en transit (TLS 1.2+) et au repos (AES-256 ou équivalent) ?	Documentation des standards de chiffrement	TOUS
C7	Les clés de chiffrement peuvent-elles être détenues ou contrôlées par le client ou par une entité exclusivement UE (BYOK/HYOK) ?	Description de l'architecture de gestion des clés	T1
C8	Publiez-vous un rapport de transparence ou une politique de réponse aux demandes gouvernementales d'accès aux données ?	URL du rapport de transparence ou politique	T1

D — Contrôle d'accès et identité

ID	Question	Preuves demandées	Niveau
D1	L'authentification multifacteur est-elle imposée pour tout accès du personnel à la production et aux données client ?	Extrait de la politique IAM ; déclaration de couverture MFA	TOUS
D2	Prenez-vous en charge le SSO (SAML/OIDC) et le provisionnement SCIM pour les tenants clients ?	Documentation sécurité du produit	T1-T2
D3	L'accès aux données client repose-t-il sur les rôles et le moindre privilège, avec un accès production restreint à un groupe nominatif ?	Politique de contrôle d'accès ; matrice des rôles	TOUS
D4	Les droits d'accès des utilisateurs sont-ils revus selon une périodicité définie (au moins trimestrielle pour les accès privilégiés) ?	Dernier compte rendu de revue des accès (caviardé)	T1-T2
D5	Les comptes à privilèges sont-ils gérés via une solution PAM avec journalisation des sessions ?	Description de l'outillage PAM	T1
D6	Votre processus arrivée/mobilité/départ révoque-t-il les accès dans un délai (SLA) défini en cas de départ ?	Description du processus avec SLA	T1-T2
D7	Effectuez-vous une vérification des antécédents des salariés ayant accès aux données client, lorsque la loi le permet ?	Déclaration de politique de vérification des antécédents	T1

E — Infrastructure et exploitation

ID	Question	Preuves demandées	Niveau
E1	Décrivez votre modèle d'hébergement (fournisseur(s) cloud, régions, mono/multi-locataire).	Vue d'ensemble de l'architecture	TOUS
E2	Les environnements de production, de recette et de développement sont-ils cloisonnés, sans aucune donnée client hors production ?	Politique d'environnements ; approche de masquage des données	T1-T2
E3	Exploitez-vous un programme de gestion des vulnérabilités avec des délais de remédiation définis pour les constats critiques ?	Politique + indicateurs de délais de correction des 6 à 12 derniers mois	TOUS
E4	Le service fait-il l'objet d'un test d'intrusion au moins annuel par un tiers indépendant, et en partagerez-vous la synthèse ?	Synthèse du dernier test d'intrusion avec état des remédiations	TOUS
E5	Les postes de travail sont-ils protégés par EDR/anti-malware, et les serveurs durcis selon un référentiel documenté ?	Description de l'outillage et du référentiel de durcissement	T1-T2
E6	Journalisez-vous de manière centralisée les événements de sécurité et les surveillez-vous (SIEM/SOC), avec une durée de rétention définie ?	Description de la journalisation/surveillance ; durée de rétention	T1-T2

ID	Question	Preuves demandées	Niveau
E7	La configuration de l'infrastructure est-elle gérée en tant que code / sous contrôle des changements avec revue par les pairs ?	Description du processus de gestion des changements	T1
E8	Disposez-vous d'une protection anti-DDoS et d'une gestion de la capacité pour les composants critiques pour la disponibilité ?	Déclaration sur le prestataire/la technologie utilisés	T1

F — Gestion et notification des incidents

ID	Question	Preuves demandées	Niveau
F1	Maintenez-vous un plan de réponse aux incidents testé, avec des rôles et des niveaux de gravité définis ?	Synthèse du plan de réponse ; date du dernier test/exercice	TOUS
F2	Mettez-vous à disposition des clients un contact incidents de sécurité 24 h/24 et 7 j/7 ?	Coordonnées / chaîne d'escalade	TOUS
F3	Quel est votre délai contractuel (en heures) de notification aux clients des incidents affectant leur service ou leurs données ?	Clause contractuelle ; doit être compatible avec l'obligation d'alerte précoce sous 24 heures de l'article 23 de NIS2 pesant sur le client	TOUS
F4	Pour les clients entités financières : pouvez-vous respecter leurs délais de déclaration des incidents majeurs DORA en fournissant l'information à temps ?	Description du processus faisant référence à l'article 19 de DORA	T1
F5	Pouvez-vous préserver et partager les preuves forensiques liées aux incidents affectant le client ?	Procédure de gestion des preuves	T1
F6	Fournissez-vous des rapports post-incident (cause racine, impact, actions correctives) aux clients affectés ?	Exemple ou modèle de rapport post-incident	T1-T2

G — Continuité d'activité et reprise après sinistre

ID	Question	Preuves demandées	Niveau
G1	Maintenez-vous des plans de continuité d'activité et de reprise après sinistre couvrant le service que nous achetons ?	Extrait du PCA/PRA	TOUS
G2	Quels sont vos RTO et RPO contractuels pour le service ?	SLA ou documentation PRA	T1-T2
G3	Les sauvegardes sont-elles chiffrées, séparées géographiquement et testées en restauration selon une périodicité définie ?	Politique de sauvegarde ; date et résultat du dernier test de restauration	TOUS
G4	Quand avez-vous testé votre PRA pour la dernière fois, et avec quels résultats ?	Synthèse du rapport de test du PRA	T1
G5	Quelles dépendances critiques (prestataires, régions, points de défaillance uniques) le service comporte-t-il ?	Déclaration sur les dépendances et concentrations	T1

H — Développement sécurisé

ID	Question	Preuves demandées	Niveau
H1	Suivez-vous un cycle de développement sécurisé documenté, avec des exigences de sécurité pour chaque version ?	Synthèse de la politique de développement sécurisé (SDLC)	T1-T2
H2	Le code est-il revu par les pairs et analysé (SAST/DAST/analyse des dépendances) avant tout déploiement en production ?	Description des contrôles de sécurité CI/CD	T1-T2
H3	Maintenez-vous un SBOM ou un inventaire des dépendances du service, et le surveillez-vous pour détecter les vulnérabilités ?	Déclaration de disponibilité du SBOM (format, périodicité)	T1
H4	Les secrets et identifiants sont-ils gérés dans un coffre-fort dédié (jamais dans les dépôts de code) ?	Description de la gestion des secrets	T1-T2
H5	Les développeurs reçoivent-ils une formation au codage sécurisé selon une périodicité définie ?	Déclaration sur le programme de formation	T1
H6	Des tests de sécurité sont-ils réalisés sur les versions majeures et les changements d'architecture ?	Processus de tests de sécurité des versions	T1

I — Sous-traitants et chaîne d'approvisionnement

ID	Question	Preuves demandées	Niveau
I1	Maintenez-vous un registre à jour des sous-traitants impliqués dans la fourniture du service, avec leurs localisations et rôles ?	Registre des sous-traitants	TOUS
I2	Vos contrats de sous-traitance répercutent-ils des obligations équivalentes en matière de sécurité et de protection des données ?	Déclaration sur les clauses de répercussion	T1-T2
I3	Évaluez-vous la sécurité de vos propres fournisseurs avant l'entrée en relation, puis selon une périodicité définie ?	Description du processus d'évaluation des fournisseurs	T1-T2
I4	Nous notifierez-vous à l'avance tout changement de sous-traitant, avec un droit d'objection ?	Clause contractuelle ; délai de préavis	TOUS
I5	Facilitez-vous la sortie du client : export des données dans un format ouvert, assistance à la migration et plan de sortie défini ?	Documentation de sortie/portabilité (cf. article 28(8) de DORA pour les entités financières)	T1-T2
I6	Pouvez-vous transmettre les preuves fournisseurs demandées au titre de nos obligations de chaîne d'approvisionnement NIS2 article 21(2)(d) ?	Déclaration d'engagement ; processus de partage des preuves	T1

J — Addendum entités financières (DORA)

ID	Question	Preuves demandées	Niveau
J1	Pouvez-vous fournir les champs de données dont les clients entités financières ont besoin pour leur registre d'informations DORA (LEI, type de service, localisation des données) ?	Fiche des champs du registre d'informations (cf. ITS (UE) 2024/2956)	T1
J2	Vos contrats portant sur des fonctions critiques ou importantes incluent-ils les dispositions de l'article 30(3) de DORA (accès, audit, résiliation, sortie) ?	Références des modèles de contrat	T1
J3	Avez-vous connaissance d'une désignation comme prestataire tiers critique de services TIC sous la supervision DORA, ou vous y préparez-vous ?	Déclaration	T1
J4	Participerez-vous aux tests de pénétration fondés sur la menace (TLPT) du client lorsque c'est requis ?	Déclaration d'engagement (cf. articles 26-27 de DORA)	T1
J5	Prenez-vous en charge des stratégies de sortie documentées, incluant l'assistance à la transition et des périodes de fonctionnement en parallèle ?	Documentation de la stratégie de sortie	T1

Du questionnaire à l'assurance continue

Un questionnaire est un instantané ; le risque fournisseur est un flux. La plateforme d'assurance fournisseurs d'Orbiq exécute en continu le même classement par niveaux, les mêmes jeux de questions, la même collecte de preuves et le même circuit de revue — avec des réponses évaluées par IA et une piste d'audit générée comme sous-produit. Voir orbiqhq.com/platform/vendor-assurance-platform.

Version 1.0 · publié le 2026-07-13 · Utilisation libre ; attribution appréciée. Source : orbiqhq.com/templates/eu-vendor-security-questionnaire