Questionnaire fournisseur NIS 2

Un questionnaire ouvert et ancré dans le droit de l'UE pour l'évaluation des fournisseurs au titre de NIS 2

Version 3.1.0 - Dernière mise à jour 2026-05-15 - 59 champs répartis en 6 sections

Chaque champ est ancré à une source primaire de niveau européen : NIS 2 Art. 21(2), CIR 2024/2690, ENISA Technical Implementation Guidance, GDPR Art. 28 ou le Cyber Resilience Act. Les compléments sectoriels (TISAX, VDA ISA, BSI C5, KRITIS) s'ajoutent à cette base.

1. Profil du fournisseur (18 champs)

Raison sociale

[string] Obligatoire - Base juridique: ENISA TIG §5.2

Le nom enregistré de votre entreprise, tel qu'il figure au registre du commerce. Exemple : Müller GmbH ou Acme Software Ltd.

Adresse du siège social

[string] Obligatoire - Base juridique: ENISA TIG §5.2

L'adresse commerciale enregistrée de votre entreprise. Une seule adresse suffit, même si vous avez plusieurs sites.

Pays

[country] Obligatoire - Base juridique: ENISA TIG §5.2

Le pays où votre entreprise est légalement établie. Deux lettres, par exemple DE pour l'Allemagne.

Domaine principal

[url] Facultatif - Base juridique: ENISA TIG §5.2(b)

Votre domaine principal, généralement l'URL de votre site web. Exemple : acmesoftware.com.

Slogan (une ligne, visible par les clients)

[string] Facultatif - Base juridique: ENISA TIG §5.2(b)

Une ligne résumant ce que vous proposez. Les clients la voient sur votre profil fournisseur. Exemple : ERP pour l'industrie manufacturière des PME.

Description publique (plus longue)

[text] Facultatif - Base juridique: ENISA TIG §5.2(b)

Deux à trois phrases sur votre entreprise et votre activité. Ce texte apparaît sur votre profil fournisseur. Argumentaire commercial, posture de sécurité, ou les deux.

Description des services fournis

[text] Obligatoire - Base juridique: ENISA TIG §5.2(b) + §5.1.4 TIPS

Un paragraphe sur ce que votre entreprise livre techniquement aux clients. Produits, modules ou services concrets. Évitez le langage purement marketing.

Pays / régions où les données des clients sont traitées

[string] Obligatoire - Base juridique: ENISA TIG §5.1.4 TIPS

Tous les pays où les données de vos clients sont stockées ou traitées. Séparés par des virgules, codes pays ISO. Exemple : DE, NL, US. Si vous traitez entièrement au sein de l'UE, lister les pays de l'UE suffit.

Nom du contact sécurité

[string] Obligatoire - Base juridique: CIR 2024/2690 §5.1.4(d)

La personne que les clients contactent lors d'un incident de sécurité. Dans les petites entreprises, souvent le directeur général ou le responsable informatique. Une seule personne suffit.

E-mail de contact pour les incidents

[email] Obligatoire - Base juridique: CIR 2024/2690 §5.1.4(d)

Adresse e-mail que les clients utilisent pour signaler un incident de sécurité. Idéalement une liste de diffusion comme security@example.com qui atteint plusieurs personnes.

Téléphone de contact pour les incidents (24/7)

[phone] Facultatif - Base juridique: CIR 2024/2690 §5.1.4(d)

Numéro de téléphone pour les signalements urgents d'incidents. Si vous n'assurez pas d'astreinte 24/7, indiquez vos heures ouvrées entre parenthèses.

SLA de notification d'incident (heures)

[integer] Facultatif - Base juridique: NIS2 Art. 23

Heures entre la détection d'un incident et la notification au client, au plus tard. Auto-évaluation réaliste, pas un objectif théorique. Valeurs courantes : 24, 48 ou 72 heures.

Identifiant d'enregistrement BSI (uniquement si votre entreprise est elle-même réglementée par NIS2)

[string] Facultatif - Base juridique: ENISA TIG §5.1.2

Si votre entreprise est elle-même soumise à NIS 2 et enregistrée auprès du BSI, saisissez ici l'identifiant d'enregistrement. Facultatif. Permet aux clients de voir d'un coup d'œil que vous remplissez la même obligation qu'une entité réglementée.

Nous fournissons des services SaaS / hébergés
[boolean] Obligatoire - Base juridique: ENISA TIG §5.2(b)
Vous exécutez des logiciels pour les clients sur votre propre infrastructure et les livrez via internet. Cochez plusieurs cases si vous proposez plusieurs modèles.

Nous livrons des logiciels on-premise
[boolean] Obligatoire - Base juridique: ENISA TIG §5.2(b)
Vous livrez des logiciels que les clients installent et exécutent sur leur propre infrastructure.

Nous fournissons des services professionnels / conseil
[boolean] Obligatoire - Base juridique: ENISA TIG §5.2(b)
Votre prestation principale est un travail humain : conseil, mise en œuvre, formation, audit ou personnalisation.

Nous fournissons des services gérés / MSP
[boolean] Obligatoire - Base juridique: ENISA TIG §5.2(b)
Vous exploitez pour le client une partie de son informatique, avec votre propre personnel. Typique des modèles MSP et MSSP.

Nous utilisons, intégrons ou fournissons des systèmes d'IA
[boolean] Obligatoire - Base juridique: NIS2 Art. 21(2)(d)
Vos produits ou services traitent-ils les données des clients via un modèle d'IA ou de ML ? Cela inclut les modèles externes que vous appelez via une API, par exemple OpenAI ou Anthropic.

2. Pratiques de sécurité (26 champs)

Système de management de la sécurité de l'information documenté (ISMS)
[boolean] Obligatoire - Base juridique: CIR 2024/2690 §5.1.2(a)
Cochez oui si vous disposez d'une politique de sécurité de l'information écrite avec des rôles attribués, des revues régulières et une gestion documentée des incidents. Une certification ISO 27001 ou BSI Grundschutz implique oui.

Détenir une certification ISO 27001, BSI Grundschutz ou équivalente
[boolean] Obligatoire - Base juridique: CIR 2024/2690 §5.1.2(b)
Cochez oui si votre entreprise détient actuellement une certification ISO 27001, BSI Grundschutz, SOC 2 Type II ou équivalente. Téléchargez le certificat dans l'onglet Certifications.

Formation annuelle de sensibilisation à la sécurité pour tout le personnel
[boolean] Obligatoire - Base juridique: CIR 2024/2690 §5.1.4(b)
Cochez oui si chaque membre du personnel reçoit au moins une formation annuelle de sensibilisation à la sécurité de l'information. Le e-learning compte ; les simulations de phishing s'y ajoutent.

Vérifications d'antécédents pour le personnel ayant accès aux données des clients
[boolean] Obligatoire - Base juridique: CIR 2024/2690 §5.1.4(c)
Cochez oui si vous effectuez une vérification d'antécédents pour le personnel ayant accès aux données des clients. Niveau courant : extrait de casier judiciaire ou document équivalent à l'embauche.

Processus documenté de gestion des vulnérabilités et de correctifs
[boolean] Obligatoire - Base juridique: CIR 2024/2690 §5.1.4(f)
Cochez oui si vous disposez d'un processus écrit pour traiter les vulnérabilités de sécurité : détecter, évaluer, prioriser, corriger ou atténuer. La surveillance des CVE et l'application de correctifs pilotée par SLA sont la norme.

Accepter le droit d'audit du client (ou fournir des rapports d'audit)
[boolean] Obligatoire - Base juridique: CIR 2024/2690 §5.1.4(e)
Cochez oui si vous accordez aux clients soit un droit d'audit sur site, soit des rapports d'audit de substitution (par exemple SOC 2, ISAE 3402).

Recours à des sous-traitants ultérieurs / sous-fournisseurs
[boolean] Obligatoire - Base juridique: CIR 2024/2690 §5.1.4(g)
Cochez oui si vous recourez à d'autres entreprises pour fournir votre service et qu'elles ont accès aux données ou à l'infrastructure des clients. Exemples typiques : AWS, Azure, Cloudflare, Stripe.

Liste des sous-traitants ultérieurs
[text] Conditionnel - Base juridique: CIR 2024/2690 §5.1.4(g)
Listez chaque sous-traitant ultérieur avec son nom, son lieu de traitement et ce qu'il fait pour vous. Un tableau ou une liste à puces suffit. Mettez-la à jour à chaque ajout ou retrait.

S'engager à restituer / détruire les données des clients à la résiliation
[boolean] Obligatoire - Base juridique: CIR 2024/2690 §5.1.4(h)
Cochez oui si vous vous engagez contractuellement à restituer ou détruire les données des clients à la fin du contrat. Pratique courante : export et restitution, puis suppression sous 30 jours.

Contrat type de traitement des données (DPA) disponible
[boolean] Obligatoire - Base juridique: GDPR Art. 28
Cochez oui si vous disposez d'un contrat type de traitement des données au titre de l'article 28 du GDPR que les clients peuvent signer. Requis dès que vous traitez des données à caractère personnel.

Politiques de sécurité revues au moins une fois par an

[boolean] Obligatoire - Base juridique: NIS2 Art. 21(2)(a) / ENISA TIG §1.1

Cochez oui si vos politiques de sécurité sont revues au moins une fois par an et mises à jour si nécessaire. Une note écrite dans le document suffit comme preuve.

Plan de réponse aux incidents documenté

[boolean] Obligatoire - Base juridique: NIS2 Art. 21(2)(b) / ENISA TIG §3

Cochez oui si vous disposez d'un plan écrit pour gérer les incidents de sécurité : qui décide, qui communique, qui documente. Au moins un exercice sur table par an est une bonne pratique.

Plan de continuité d'activité / reprise après sinistre documenté

[boolean] Obligatoire - Base juridique: NIS2 Art. 21(2)(c) / ENISA TIG §4

Cochez oui si vous disposez d'un plan expliquant comment vous maintenez l'activité ou récupérez rapidement lors d'une panne : systèmes critiques, solutions de repli, objectifs RTO et RPO.

Politique de cryptographie documentée

[boolean] Obligatoire - Base juridique: NIS2 Art. 21(2)(h) / ENISA TIG §9

Cochez oui si vous avez consigné par écrit quelle cryptographie vous utilisez et où : données en transit (TLS 1.2+), données au repos (AES-256), gestion des clés, algorithmes de hachage.

Gestion des accès à privilèges (PAM) pour le personnel interne

[boolean] Obligatoire - Base juridique: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Cochez oui si les administrateurs et les comptes à privilèges bénéficient de contrôles supplémentaires : connexion distincte, MFA, journalisation des sessions ou accès juste-à-temps.

MFA imposé pour tous les comptes d'administration / à privilèges internes

[boolean] Obligatoire - Base juridique: NIS2 Art. 21(2)(j)

Cochez oui si chaque compte d'administration ou à privilèges interne doit utiliser le MFA. Les jetons matériels ou les applications d'authentification comptent ; le SMS ne compte pas.

Tenir un inventaire des actifs d'information

[boolean] Obligatoire - Base juridique: NIS2 Art. 21(2)(i) / ENISA TIG §12.4

Cochez oui si vous tenez une liste à jour de chaque système d'information que vous utilisez pour fournir votre service : serveurs, bases de données, outils SaaS, terminaux. Un tableur suffit.

Programme de tests d'intrusion annuel ou biennal

[boolean] Obligatoire - Base juridique: NIS2 Art. 21(2)(e) / ENISA TIG §6.5

Cochez oui si vous commandez un test d'intrusion externe au moins tous les un à deux ans. Pour les petites entreprises, un scan de vulnérabilités externe comme étape minimale est acceptable.

Nous divulguons les événements de cybersécurité notifiables passés à la demande des clients

[boolean] Obligatoire - Base juridique: ENISA TIG §5.1.2

Cochez oui si, à la demande du client, vous divulguez ouvertement si et quels incidents de sécurité à signaler votre entreprise a connus par le passé. Fenêtre courante : les trois à cinq dernières années.

Fournir une assistance aux clients en cas d'incident sans frais / à coût défini à l'avance

[boolean] Obligatoire - Base juridique: ENISA TIG §5.1.4 TIPS

Cochez oui si vous vous engagez à aider les clients sans frais supplémentaires lorsqu'un incident est causé par votre produit ou service. Si vous convenez plutôt d'un tarif journalier défini à l'avance, cochez également oui.

Coopérer pleinement avec les autorités compétentes (BSI, ENISA, CSIRT nationaux)

[boolean] Obligatoire - Base juridique: ENISA TIG §5.1.4 TIPS

Cochez oui si vous vous engagez à coopérer pleinement avec les autorités compétentes telles que le BSI, l'ENISA ou les CSIRT nationaux lors des inspections, des audits et du traitement des incidents. Standard pour les fournisseurs sérieux.

Informer les clients de tout changement important affectant la prestation du service

[boolean] Obligatoire - Base juridique: ENISA TIG §5.1.4 TIPS

Cochez oui si vous vous engagez à informer les clients de tout changement important affectant votre capacité à fournir le service : acquisitions, changements de sous-traitant ultérieur, évolutions techniques majeures.

Informer les clients à l'avance en cas de changement des lieux de traitement des données

[boolean] Obligatoire - Base juridique: ENISA TIG §5.1.4 TIPS

Cochez oui si vous informez les clients à l'avance avant que le lieu de traitement de leurs données ne change. Important pour la protection des données et pour une supervision de la chaîne d'approvisionnement conforme au GDPR.

Stratégie de sortie documentée avec période de transition obligatoire

[boolean] Obligatoire - Base juridique: ENISA TIG §5.1.4 TIPS

Cochez oui si vous disposez d'une stratégie de sortie écrite : combien de temps dure une passation ordonnée, quelles données et connaissances sont transférées, à quoi vous vous engagez pendant la transition.

Fournir un SBOM-for-AI selon les éléments minimaux du G7

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2

Facultatif. Cochez oui si vous pouvez fournir un SBOM-for-AI selon les éléments minimaux du G7 (mai 2026). Documente les métadonnées, les modèles, les données d'entraînement, l'infrastructure, les propriétés de sécurité, les KPI et le comportement du système. Standard volontaire.

URL du document SBOM-for-AI

[url] Conditionnel - Base juridique: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2

URL publique ou partagée vers votre document SBOM-for-AI. Peut être un PDF, un fichier JSON ou une page de projet.

3. Spécifique au SaaS (5 champs)

Région d'hébergement

[string] Conditionnel - Base juridique: ENISA TIG §5.2

La région cloud où les données des clients sont hébergées. Exemple : AWS eu-central-1, Azure West Europe. Indiquez la région principale ; les régions secondaires ou de sauvegarde peuvent être ajoutées séparées par des virgules.

Chiffrement au repos

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(h) / ENISA TIG §9

Cochez oui si les données des clients sur disque sont chiffrées au repos avec AES-256 ou équivalent. Le chiffrement de disque géré par le cloud (AWS EBS, Azure Disk Encryption) compte.

Chiffrement en transit (TLS "e 1.2)

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(h) / ENISA TIG §9

Cochez oui si tous les points d'accès exposés aux clients imposent TLS 1.2 ou supérieur. TLS 1.3 est préférable. Le HTTP simple doit rediriger vers HTTPS.

MFA imposé pour tous les comptes d'administration

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(j) / ENISA TIG §11.3

Cochez oui si chaque compte d'administration interne sur la plateforme SaaS doit utiliser le MFA. Même standard que votre politique d'administration interne.

Objectif de temps de reprise (RTO) en heures

[integer] Conditionnel - Base juridique: NIS2 Art. 21(2)(c) / ENISA TIG §4

Nombre maximal d'heures pendant lesquelles votre service peut être indisponible avant reprise. Valeur SLA réaliste, pas un objectif théorique. Valeurs SaaS courantes : 4, 8 ou 24 heures.

4. Spécifique à l'On-Premise (4 champs)

Fournir une nomenclature logicielle (SBOM)

[boolean] Conditionnel - Base juridique: CRA / NIS2 Art. 21(2)(d)

Cochez oui si vous livrez une nomenclature logicielle (SBOM) avec chaque version. CycloneDX ou SPDX sont les formats standard. Obligatoire au titre du Cyber Resilience Act pour les produits mis sur le marché de l'UE à partir de décembre 2027.

Les versions sont signées cryptographiquement

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(e) / ENISA TIG §6.5

Cochez oui si chaque artefact de version porte une signature cryptographique que les clients peuvent vérifier. Les clés de signature sont documentées et font l'objet d'une rotation. Les signatures Sigstore ou PGP comptent toutes les deux.

Politique de divulgation des vulnérabilités publiée

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(e) / ENISA TIG §3

Cochez oui si vous disposez d'un moyen documenté publiquement pour signaler les vulnérabilités de sécurité. Un fichier security.txt sur votre domaine (selon RFC 9116) ou une adresse e-mail dédiée comme security@example.com suffit.

SLA de correctif pour les CVE critiques (heures)

[integer] Conditionnel - Base juridique: CIR 2024/2690 §5.1.4(f)

Heures entre la divulgation publique d'une CVE et une version corrigée pour les vulnérabilités critiques (CVSS 9.0+). Engagement réaliste, pas un objectif théorique. Valeurs courantes : 24, 48 ou 72 heures.

5. Professional Services (3 champs)

Portée des vérifications d'antécédents

[string] Conditionnel - Base juridique: NIS2 Art. 21(2)(i) / CIR 2024/2690 §5.1.4(c)

Décrivez comment vous évaluez les consultants pour les rôles sensibles. Exemple : extrait de casier judiciaire pour tous les consultants, ainsi que des vérifications de références pour les missions impliquant des données classifiées.

NDA conclu avec tous les consultants

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(i) / ENISA TIG §11.4

Cochez oui si chaque consultant signe un accord de confidentialité avant d'être affecté à une mission client. Soit dans le cadre du contrat de travail, soit sous la forme d'un NDA distinct.

Politique de comportement documentée sur le site du client

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Cochez oui si vous disposez d'un code de conduite écrit pour les consultants travaillant sur le site du client : gestion des badges, règle de verrouillage de l'écran, conduite à tenir si des données quittent le site.

6. Managed Services (3 champs)

Gestion des accès à privilèges (PAM) en place

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Cochez oui si vous utilisez un outil de gestion des accès à privilèges pour les sessions distantes d'administration sur les systèmes des clients. Exemples : CyberArk, BeyondTrust, Teleport. Une configuration de jump-host journalisée compte.

Les sessions d'administration sont enregistrées

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(f) / ENISA TIG §10

Cochez oui si les sessions d'administration sur les systèmes des clients sont enregistrées et conservées à des fins de vérification. Conservation courante : 90 jours à 1 an. Nécessaire pour la reconstruction forensique après un incident.

Astreinte 24/7

[boolean] Conditionnel - Base juridique: NIS2 Art. 21(2)(b) / ENISA TIG §3

Cochez oui si vous assurez une astreinte 24/7 qui répond aux incidents de sécurité sur les systèmes des clients. Un support limité aux heures ouvrées ne suffit pas.