



Contrat de sous-traitance

Traitement des données à caractère personnel — article 28 du Règlement (UE) 2016/679

Élément	Valeur
Référence	DPA-DOKSURE-2026-10
Version	1.0
Date	Octobre 2026
Objet	Encadrement des traitements de données à caractère personnel réalisés par LSP Labs pour le compte du Responsable de traitement dans le cadre du Service Doksure.
Contrat principal	Conditions générales d'utilisation, bon de commande ou contrat d'abonnement applicable.
Durée	Durée du Contrat principal.
Droit applicable	Droit français.
Contact	hello@doksure.com — objet « RGPD/Violation ».

ENTRE LES SOUSSIGNÉS :

LSP Labs SAS, société par actions simplifiée immatriculée au Registre du commerce et des sociétés de Paris, SIREN 935 092 148, RCS Paris, dont le siège social est situé 60 rue François Premier, 75008 Paris, France, représentée par [nom, prénom et fonction], ci-après « **le Sous-traitant** » ;

ET

[Raison sociale du Responsable de traitement], [forme juridique], immatriculée sous le numéro [SIREN], dont le siège social est situé [adresse complète], représentée par [nom, prénom et fonction], ci-après « **le Responsable de traitement** » ;

ci-après ensemble « **les Parties** ».

Le présent Contrat complète le Contrat principal et s'applique aux Traitements réalisés par LSP Labs pour le compte du Responsable de traitement. Il prévaut sur le Contrat principal en cas de contradiction relative à la protection des Données. Il est établi par écrit, y compris sous forme électronique.

L'essentiel

- Doksure agit comme sous-traitant, sur instructions documentées.
- Documents chiffrés côté client, AES-256, hébergés dans l'UE ; LSP Labs ne détient pas les clés.
- Sous-traitants limités à l'annexe 2 ; tout changement est notifié et peut être contesté.
- Violations notifiées sans retard injustifié ; fin de Contrat : restitution ou suppression. Service non certifié HDS.

1. Objet et champ d'application

- 1.1. Le Contrat encadre les Traitements réalisés par LSP Labs, Sous-traitant, pour le compte du Responsable de traitement dans le Service Doksure, conformément à l'article 28 du RGPD et à la Loi Informatique et Libertés.
- 1.2. Il s'applique aux Traitements décrits à l'annexe 1 ; les annexes 1 et 2 font partie intégrante du Contrat.
- 1.3. Le Responsable de traitement détermine les finalités et moyens essentiels et a choisi le Sous-traitant au vu de garanties suffisantes.
- 1.4. Le Contrat ne régit pas les Traitements pour lesquels LSP Labs agit comme responsable de traitement (site, prospection, facturation, sécurité), régis par la Politique de confidentialité.

2. Définitions

- 2.1. « **RGPD** » : Règlement (UE) 2016/679 ; « **Loi Informatique et Libertés** » : loi n° 78-17 du 6 janvier 1978 modifiée. 2.2. Termes non définis : sens de l'article 4 du RGPD.
- 2.3. « **Données** » : données à caractère personnel traitées pour le compte du Responsable de traitement (annexe 1). 2.4. « **Service** » : la solution en ligne Doksure (app.doksure.com).
- 2.5. « **Sous-traitant ultérieur** » : entité traitant des Données pour le compte du Sous-traitant. 2.6. « **Violation** » : violation de la sécurité entraînant destruction, perte, altération, divulgation ou accès non autorisé à des Données.
- 2.7. « **Contrat principal** » : les CGU, le bon de commande ou le contrat d'abonnement. 2.8. « **EEE** » : Espace économique européen. « **CCT** » : clauses de la décision (UE) 2021/914.

3. Traitement et instructions

- 3.1. Le Responsable de traitement est seul responsable de la licéité, des bases légales, de l'information des personnes, des consentements, de la minimisation et des durées de conservation.
- 3.2. Le Sous-traitant ne traite les Données que sur instructions documentées, y compris pour les transferts hors EEE, sauf obligation légale de l'Union ou d'un État membre ; il en informe alors le Responsable de traitement avant le Traitement, sauf interdiction légale.
- 3.3. Le Sous-traitant informe immédiatement le Responsable de traitement si une instruction lui paraît enfreindre le RGPD ou d'autres dispositions relatives à la protection des données.
- 3.4. Il ne traite pas les Données à d'autres fins que celles de l'annexe 1, ne les vend pas et ne les communique qu'au Responsable de traitement, à ses utilisateurs autorisés et aux sous-traitants ultérieurs, sauf obligation légale ou instruction écrite.

3.5. Il tient un registre des activités de Traitement (article 30, paragraphe 2, du RGPD).

4. Confidentialité du personnel

4.1. Le Sous-traitant veille à ce que les personnes autorisées s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée ; l'accès est limité au personnel qui en a besoin.

4.2. Il sensibilise et forme son personnel, révoque les accès en cas de départ et veille à la restitution des supports. La confidentialité survit à la fin du Contrat.

5. Sécurité

5.1. Le Sous-traitant met en œuvre les mesures de l'annexe 1 et toute mesure nécessaire au niveau de sécurité adapté au risque (article 32 du RGPD).

5.2. Ces mesures comprennent le chiffrement côté client, AES- 256 au repos et en transit, le hachage des mots de passe, l'authentification à deux facteurs, le contrôle des accès, la journalisation et l'hébergement dans l'Union européenne.

5.3. LSP Labs ne détient pas les clés et ne conserve pas le mot de passe ; il ne peut donc ni déchiffrer les documents ni restaurer un mot de passe.

5.4. Le Responsable de traitement sécurise ses accès et ceux de ses utilisateurs : mots de passe robustes, authentification à deux facteurs, habilitations et terminaux.

5.5. Le Service n'est pas un hébergement certifié HDS ; les données de santé soumises à cette certification exigent un accord écrit spécifique préalable.

6. Sous-traitants ultérieurs

6.1. Le Responsable de traitement autorise de manière générale le recours aux sous-traitants ultérieurs de l'annexe 2.

6.2. Aucun autre sous-traitant ultérieur n'est autorisé sans accord écrit préalable.

6.3. Tout ajout ou remplacement est notifié trente (30) jours avant son entrée en vigueur, avec l'identité, les services, les Données, la localisation et les garanties ; le Responsable de traitement peut s'y opposer dans les trente (30) jours, puis résilier la partie concernée sans pénalité à défaut d'accord.

6.4. Le Sous-traitant impose contractuellement des obligations au moins équivalentes à chaque sous-traitant ultérieur et demeure entièrement responsable de leur exécution.

6.5. La liste de l'annexe 2 est mise à jour à chaque changement.

7. Droits des personnes et coopération

- 7.1. Le Sous-traitant aide le Responsable de traitement, dans la mesure du possible, à répondre aux demandes des personnes concernées au titre du chapitre III du RGPD.
- 7.2. Lorsqu'une personne concernée adresse une demande au Sous-traitant, celui-ci la transmet sans délai au Responsable de traitement et ne répond pas sur le fond, sauf instruction écrite ou obligation légale.
- 7.3. Le Sous-traitant assiste le Responsable de traitement, dans la mesure du possible, pour l'analyse d'impact (article 35) et les consultations préalables (article 36).
- 7.4. Les demandes excessives peuvent être facturées après accord écrit.

8. Violations

- 8.1. Le Sous-traitant notifie toute Violation sans retard injustifié après en avoir pris connaissance et fournit les informations dont il dispose, complétées progressivement.
- 8.2. La notification précise, dans la mesure disponible, la nature de la Violation, les catégories et le nombre approximatif de personnes et de documents concernés, la date, les conséquences probables, les mesures prises et les services concernés.
- 8.3. Le Sous-traitant coopère pour évaluer, contenir et atténuer la Violation. Il appartient au Responsable de traitement de notifier l'Autorité de contrôle et les personnes concernées ; la notification ne vaut pas reconnaissance de responsabilité.

9. Audit et preuve de conformité

- 9.1. Le Sous-traitant met à disposition les informations nécessaires pour démontrer le respect de l'article 28 du RGPD et permettre les audits, y compris des inspections, du Responsable de traitement ou d'un auditeur mandaté.
- 9.2. Le Responsable de traitement peut auditer le Sous-traitant une fois par an, à ses frais, après préavis raisonnable, sans perturber le Service et sous réserve de confidentialité.
- 9.3. Le rapport d'audit est confidentiel ; les preuves sont conservées pendant la durée du Contrat et la prescription applicable.

10. Sort des données

- 10.1. Le Responsable de traitement peut exporter les Données à tout moment dans un format structuré et couramment utilisé.

- 10.2.** À la fin du Contrat principal, le Sous-traitant restitue ou supprime les Données et leurs copies, au choix du Responsable de traitement.
- 10.3.** La restitution ou la suppression intervient dans les trente (30) jours ; une attestation est délivrée sur demande.
- 10.4.** Si la loi impose la conservation de Données, le Sous-traitant en informe le Responsable de traitement et en limite l'accès. **10.5.** Il appartient au Responsable de traitement d'exporter les documents et de conserver ses clés avant la fin du Contrat.

11. Transferts hors EEE

- 11.1.** Les Données sont hébergées dans l'Union européenne ; aucun transfert hors EEE n'a lieu sans instruction documentée ou obligation légale.
- 11.2.** Tout transfert nécessaire est encadré par les CCT, module 2 ou 3, complétées par des mesures supplémentaires adaptées.
- 11.3.** Aucune décision d'adéquation n'est présumée ; elle ne s'applique que si elle est en vigueur et couvre le transfert.

12. Responsabilité, durée, droit applicable et signature

- 12.1.** La responsabilité du Sous-traitant est soumise aux limitations du Contrat principal, sans préjudice des articles 28, paragraphe 10, et 82 du RGPD.
- 12.2.** Le Contrat prend effet à sa signature et dure autant que le Contrat principal.
- 12.3.** Toute modification requiert un avenant écrit. **12.4.** Le Contrat est régi par le droit français ; tout litige relève des tribunaux compétents de Paris. **12.5.** Le Contrat peut être signé manuscritement ou électroniquement conformément au règlement (UE) n° 910/2014 (eIDAS).

Pour le Sous-traitant	Pour le Responsable de traitement
LSP Labs SAS	[Raison sociale du Responsable de traitement]
Nom : [nom, prénom]	Nom : [nom, prénom]
Fonction : [fonction]	Fonction : [fonction]
Date : [date]	Date : [date]
Lieu : [lieu]	Lieu : [lieu]
Signature :	Signature :

Annexe 1 — Traitement et mesures de sécurité

A. Description du traitement

Élément	Description
Objet	Mise à disposition du Service Doksure pour collecter, stocker, consulter, partager et exporter des documents, gérer les comptes et les accès.
Nature et finalités	Collecte, enregistrement, conservation, consultation, communication et effacement. Finalités : gérer les demandes, collecter et stocker les documents, envoyer notifications et relances, gérer les comptes et accès, journaliser les accès et assurer le support.
Catégories de Données	Identité et contact (nom, prénom, e-mail, téléphone, entreprise, fonction) ; compte (identifiant, mot de passe haché) ; documents déposés (pièces d'identité, justificatifs de domicile, documents fiscaux, contrats) ; demande (objet, type de pièces, statut, messages) ; données techniques (adresse IP, navigateur, horodatages, journaux d'accès). Le Service n'est pas destiné aux données de l'article 9 du RGPD ; les données de santé HDS sont exclues (article 5.5).
Personnes concernées	Clients, prospects et contacts ; représentants et collaborateurs autorisés ; personnes dont les documents sont déposés, notamment clients, patients ou salariés.
Durée	Durée du Contrat principal ; restitution ou suppression dans les trente (30) jours.
Destinataires	LSP Labs, ses sous-traitants ultérieurs (annexe 2), les utilisateurs autorisés et les destinataires de liens.

B. Mesures techniques et organisationnelles

Domaine	Mesures
Chiffrement	Chiffrement côté client, AES-256 au repos et en transit. Les hébergeurs ne reçoivent que des données chiffrées.
Clés et mots de passe	Mots de passe hachés. Clés dérivées du mot de passe, non stockées par LSP Labs, qui ne peut ni déchiffrer les documents ni restaurer un mot de passe.
Accès et authentification	Identifiant et mot de passe, authentification à deux facteurs, espaces distincts par client, liens protégés.
Journalisation	Historique des accès (qui a ouvert quel document et quand).
Hébergement	Hébergement dans l'Union européenne auprès de Cloudflare, Inc. et d'OVH ; les hébergeurs ne reçoivent que des données chiffrées.
Incidents	Notification des Violations (article 8).
Personnel	Confidentialité et gestion des accès.

La Politique de confidentialité décrit les traitements pour lesquels LSP Labs agit comme responsable de traitement ; elle ne se substitue pas à la présente annexe pour les Traitements réalisés pour le compte du Responsable de traitement.

Annexe 2 — Sous-traitants ultérieurs autorisés

La liste reprend celle publiée dans la Politique de confidentialité à la date du Contrat ; elle ne peut être modifiée que conformément à l'article 6.

Sous-traitant ultérieur	Finalité	Localisation des données
PostHog	Analyse de l'utilisation du Site et de l'application	Union européenne — endpoint UE uniquement, aucun transfert vers les États-Unis
Crisp	Chat en direct et support client	Union européenne (Pays-Bas)
Stripe	Traitement des paiements	Union européenne
Chargebee	Gestion des abonnements et des paiements récurrents	Union européenne — endpoint UE
Cloudflare, Inc.	Stockage des données et sécurisation du Site	Union européenne — endpoints européens
OVH	Stockage des données et sécurisation du Site	Europe — serveurs situés en Europe

Les sous-traitants de stockage ne reçoivent que des données chiffrées. Tout ajout ou remplacement est notifié trente (30) jours avant son entrée en vigueur (article 6.3).