CONTRAT DE SOUS-TRAITANCE

Data Processing Agreement (DPA)

conformément à l'article 28 du RGPD (UE) 2016/679

entre

Nom et coordonnées du Client

— Responsable de traitement au sens du RGPD, ci-après « le Client » —

et

LRob SARL

représentée par Robin LABADIE, gérant

23, rue Alexandre Antigna – 45000 Orléans – France

SIREN 105 115 554 – RCS Orléans – Capital social : 2 048,00 €

abuse@lrob.net | www.lrob.fr | 02 21 827 827

— Sous-traitant au sens du RGPD, ci-après « LRob » —

Version 1.0 – juin 2026

Document public – Template disponible sur lrob.fr

Introduction

Le présent Contrat de Sous-traitance (ci-après « DPA ») définit les obligations en matière de protection des données des parties contractantes, ainsi que les traitements de données à caractère personnel réalisés dans le cadre du contrat principal conclu entre le Client et LRob.

Le DPA s'applique à toutes les activités relevant du contrat principal dans le cadre desquelles des données à caractère personnel sont traitées par LRob ou des tiers qu'il mandate, pour le compte du Client.

§ 1 – Objet et durée

(1) Le présent DPA définit les obligations des parties en matière de protection des données dans le cadre du traitement de données personnelles résultant du contrat principal. Ce contrat principal est constitué des services d'hébergement web, d'hébergement Nextcloud, d'infogérance et/ou de webmastering souscrits par le Client auprès de LRob, tels que décrits dans les CGV (pour les commandes via le portail lrob.fr) ou dans le devis signé.

(2) LRob traitera des données à caractère personnel pour le compte du Client conformément à l'art. 4 n° 2 du RGPD dans le cadre du présent DPA.

(3) Dans le cadre du présent DPA, le Client est seul responsable de la conformité à la réglementation applicable en matière de protection des données. En particulier, le Client s'assurera que le transfert de données à LRob et leur traitement sont licites. Le Client est considéré comme « responsable du traitement » au sens de l'art. 4 n° 7 du RGPD.

(4) Le présent DPA est subordonné à l'existence de la relation contractuelle principale visée au § 1(1). La résiliation ou toute autre extinction du contrat principal entraîne simultanément la fin du présent DPA.

§ 2 – Objet, nature et finalité du traitement

L'objet, la nature et la finalité du traitement, ainsi que la nature des données et les catégories de personnes concernées, sont décrits à l'Annexe 1 du présent DPA, complétée par le Client. Pour les services standards d'hébergement, les éléments suivants constituent une description générique applicable par défaut :

Description générale du traitement (par défaut)	
Finalité	Hébergement des données et fichiers du Client dans le cadre de la fourniture des services contractuels (hébergement web, Nextcloud, messagerie, bases de données, infogérance)
Nature des opérations	Stockage, sauvegarde, transmission, mise à disposition
Catégories de données	Données des visiteurs/utilisateurs du site Client, données de connexion, contenu hébergé, données de messagerie, bases de données applicatives
Personnes concernées	Clients et visiteurs du Client, collaborateurs du Client
Durée	Durée du contrat principal + 30 jours après résiliation (délai de suppression des données hébergées actives)

§ 3 – Transferts hors Union européenne

(1) Le traitement des données contractuellement défini est réalisé exclusivement dans un État membre de l'Union européenne ou dans un autre État partie à l'Accord sur l'Espace économique européen.

(2) Certains sous-traitants ultérieurs listés à l'Annexe 3 peuvent traiter des données hors UE (ex. : Stripe, OpenAI/Anthropic, hCaptcha, Cloudflare – USA). Ces transferts sont encadrés par des clauses contractuelles types (SCC) ou décisions d'adéquation conformément aux art. 44 et suivants du RGPD.

(3) LRob informera préalablement le Client de tout changement concernant ces transferts et les garanties mises en place. LRob s'engage à fournir la preuve des garanties mises en œuvre sur demande.

§ 4 – Mesures techniques et organisationnelles (TOMs)

(1) LRob met en œuvre des mesures techniques et organisationnelles conformément à l'art. 32 du RGPD afin d'assurer un niveau de protection adapté au risque. Ces mesures garantissent en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services liés au traitement des données.

(2) Les mesures techniques et organisationnelles sont soumises au progrès technique. LRob est autorisé à mettre en œuvre des mesures alternatives adéquates, à condition que le niveau de sécurité décrit en Annexe 2 ne soit pas diminué. Toute modification substantielle doit être documentée.

(3) La description détaillée des TOMs actuellement en vigueur figure à l'Annexe 2 du présent DPA.

§ 5 – Obligations de LRob (Sous-traitant)

LRob confirme avoir connaissance des réglementations applicables en matière de protection des données et s'engage à respecter les principes d'un traitement approprié des données. LRob garantit en particulier le respect des obligations suivantes :

1. Référent protection des données

LRob n'a pas désigné de DPO (seuil légal non atteint). Le référent en matière de protection des données est Robin LABADIE, gérant, joignable à abuse@lrob.net ou au 02 21 827 827 (lun–ven 9h30–12h30 / 14h–18h).

2. Confidentialité

LRob ne confie le traitement défini dans le présent DPA qu'à des intervenants tenus à la confidentialité et préalablement sensibilisés aux règles applicables. Cette obligation de confidentialité persiste après la fin du contrat principal.

3. Mise en œuvre des TOMs

LRob s'engage à mettre en œuvre et à respecter l'ensemble des mesures techniques et organisationnelles décrites à l'Annexe 2 du présent DPA.

4. Coopération avec l'autorité de contrôle

LRob coopérera, sur demande, avec la CNIL dans le cadre de l'exercice de ses missions. LRob informera immédiatement le Client de toute inspection ou mesure de l'autorité de contrôle le concernant, sauf obligation légale de confidentialité.

5. Assistance lors de procédures réglementaires

Dans la mesure où le Client est soumis à une inspection de l'autorité de contrôle, à une procédure administrative ou pénale, ou à une réclamation d'une personne concernée en lien avec le traitement effectué par LRob, celui-ci mettra tout en œuvre pour assister le Client dans la limite de ses moyens.

6. Audits réguliers des TOMs

LRob contrôle régulièrement ses processus internes ainsi que l'efficacité de ses mesures techniques et organisationnelles.

7. Assistance pour les demandes des personnes concernées

LRob assistera raisonnablement le Client dans le traitement des demandes des personnes concernées au titre du Chapitre III du RGPD. Si une personne concernée contacte directement LRob, celui-ci réfèrera la demande au Client dans les meilleurs délais et au plus tard sous 5 jours ouvrables.

8. Notification des violations de données

LRob informera le Client sans délai, et au plus tard dans les 48 heures suivant la détection, de toute violation de données à caractère personnel affectant les données du Client. Cette notification comprendra au minimum :

- une description de la nature de la violation, y compris les catégories et le nombre approximatif de personnes concernées et d'enregistrements affectés ;
- les coordonnées du référent protection des données ;
- une description des conséquences probables de la violation ;
- une description des mesures prises ou envisagées pour remédier à la violation.

§ 6 – Obligations du Client (Responsable de traitement)

Le Client informera immédiatement et complètement LRob s'il constate des erreurs ou irrégularités dans les résultats de ses données traitées.

Le Client est seul responsable de la licité des traitements qu'il confie à LRob, de l'information des personnes concernées, et de la conformité des données hébergées aux réglementations applicables.

Le Client s'assurera que les instructions données à LRob sont conformes au RGPD et à la réglementation applicable.

§ 7 – Sous-traitants ultérieurs

(1) Constituent des sous-traitants ultérieurs au sens du présent DPA les services directement liés à la fourniture de la prestation principale. Ne sont pas concernés les services annexes tels que les télécommunications ou les services de transport.

(2) Le Client consent à ce que LRob fasse appel aux sous-traitants ultérieurs listés à l'Annexe 3 du présent DPA. LRob informera le Client dans un délai raisonnable de 14 jours avant tout ajout ou remplacement d'un sous-traitant.

(3) Le Client dispose d'un droit d'opposition dans le délai de 14 jours. En l'absence d'opposition dans ce délai, le changement est réputé accepté. En cas d'opposition légitime non résolue, le Client pourra résilier son contrat principal dans les conditions prévues par les CGV.

(4) LRob impose à ses sous-traitants ultérieurs des obligations de protection des données équivalentes à celles du présent DPA.

§ 8 – Droits d'audit du Client

(1) LRob donnera au Client des moyens appropriés de vérifier le respect des obligations du présent DPA. LRob s'engage à fournir, sur demande écrite, toutes les informations pertinentes, notamment : journaux d'accès, preuves de configuration de sécurité, documentation des TOMs.

(2) Les audits sont réalisés exclusivement par voie documentaire ou à distance. LRob ne disposant pas de locaux professionnels dédiés, aucune visite physique ne peut être exigée. Pour ce qui concerne la sécurité physique des serveurs, le Client est renvoyé aux audits et certifications de l'hébergeur infrastructure (Hetzner Online GmbH – ISO 27001, BSI C5 Type 2), dont la documentation est disponible à l'adresse https://accounts.hetzner.com/account/dpa.

(3) LRob peut démontrer sa conformité notamment par : la fourniture de la documentation des TOMs (Annexe 2), les certifications de l'hébergeur infrastructure, ou tout rapport d'évaluation tiers le cas échéant.

(4) Les prestations d'audit allant au-delà d'une demande documentaire par an sont facturées au taux horaire applicable selon les CGV.

§ 9 – Assistance complémentaire

(1) LRob assistera le Client dans le respect de ses obligations découlant des articles 32 à 36 du RGPD, notamment : mise en œuvre de mesures de sécurité appropriées, notification des violations, information des personnes concernées, réalisation d'analyses d'impact (AIPD), consultation préalable auprès de la CNIL.

(2) LRob pourra facturer les prestations d'assistance allant au-delà de ses obligations légales ou résultant d'actions ne relevant pas d'une faute de sa part. Les tarifs applicables sont ceux figurant dans les CGV ou le devis.

§ 10 – Instructions du Client

(1) LRob et ses intervenants ne traiteront les données personnelles soumises au présent DPA que dans le cadre du contrat principal et conformément aux instructions documentées du Client, sauf obligation légale contraire.

(2) Les instructions initiales du Client sont définies par le présent DPA. Le Client peut les modifier, compléter ou remplacer par écrit (y compris par courriel). Les instructions orales doivent être confirmées par écrit sans délai.

(3) LRob informera immédiatement le Client s'il estime qu'une instruction viole le RGPD ou toute autre réglementation applicable. LRob sera en droit de suspendre l'exécution de cette instruction jusqu'à confirmation ou modification par le Client.

§ 11 – Suppression et restitution des données

(1) Aucune copie ou duplication des données ne sera créée sans la connaissance du Client, exception faite des sauvegardes nécessaires au bon fonctionnement du service (décrites à l'Annexe 2) et des données requises par des obligations légales de conservation.

(2) À la demande écrite du Client ou à l'expiration du contrat principal, les données hébergées actives du Client sont supprimées dans un délai de 30 jours. Le Client peut récupérer l'intégralité de ses données (fichiers + dump SQL) via lien sécurisé ou support fourni par le Client avant cette échéance.

(3) Après suppression des données actives, des données résiduelles peuvent subsister dans les sauvegardes techniques pendant la durée de leur cycle de rétention : jusqu'à 3 mois pour les sauvegardes Plesk (Storage Box Hetzner) et jusqu'à 1 an pour les sauvegardes système (BackupPC). Ces rétentions résiduelles constituent une nécessité technique documentée et ne constituent pas un traitement actif des données du Client. L'accès à ces sauvegardes est restreint à LRob.

(4) Les données liées au compte client (facturation, tickets) sont conservées par LRob pendant 5 ans après la dernière commande à des fins comptables et de gestion des litiges. Les logs serveur sont conservés 3 ans. Ces rétentions internes ne concernent pas les données hébergées du Client.

(5) Les sauvegardes réalisées par LRob constituent une mesure de résilience technique au titre de l'art. 32 RGPD. Elles ne se substituent pas aux obligations propres du Client en matière de sauvegarde de ses données applicatives. La responsabilité de la conservation des données du Client incombe au Client.

(6) LRob conservera la documentation attestant du traitement correct des données après la fin du contrat, pour la durée des délais de conservation applicables.

§ 12 – Dispositions diverses

12.1 Droit applicable

Le présent DPA est régi par le droit français. Le tribunal compétent pour tout litige est celui d'Orléans, sans préjudice des dispositions protectrices applicables au consommateur.

12.2 Responsabilité

Le régime de responsabilité convenu dans le contrat principal s'applique également au présent DPA. La responsabilité globale de LRob est plafonnée conformément aux CGV.

12.3 Prévalence

En cas de contradiction entre les dispositions du présent DPA et celles du contrat principal, les dispositions du présent DPA en matière de protection des données prévaudront.

12.4 Modifications

Toute modification au présent DPA doit faire l'objet d'un accord écrit (y compris électronique). Il doit être expressément mentionné qu'il s'agit d'un avenant au présent DPA.

12.5 Clause de divisibilité

Si une disposition du présent DPA est déclarée invalide, les autres dispositions restent pleinement en vigueur.

Acceptation

Le présent DPA fait partie intégrante des Conditions Générales de Vente (CGV) de LRob, disponibles à l'adresse www.lrob.fr/cgv/. L'acceptation des CGV par le Client, que ce soit par commande via le portail lrob.fr ou par signature d'un devis, vaut acceptation du présent DPA.

Le présent DPA entre en vigueur à la date de conclusion du contrat principal et reste applicable pendant toute la durée de la relation contractuelle.

La version en vigueur du présent DPA est celle publiée à l'adresse www.lrob.fr/dpa/ à la date de conclusion du contrat principal. LRob se réserve le droit de mettre à jour le présent DPA pour refléter l'évolution de ses pratiques ou de la réglementation. Toute modification substantielle sera notifiée au Client conformément aux CGV.

Annexe 1 – Description du traitement

À compléter par le Client. Les informations ci-dessous constituent le cadre par défaut applicable aux services standards.

Description du traitement	
Finalité principale	À compléter par le Client
Nature des opérations	Stockage, sauvegarde, transmission, mise à disposition
Types de données traitées	• Données maîtresses personnelles • Données de communication (emails) • Données de navigation / logs • Données du contrat et de facturation • Contenu hébergé (fichiers, bases de données) • Autres : _____
Personnes concernées	• Clients et visiteurs du Client • Collaborateurs du Client • Autres : _____
Durée du traitement	Durée du contrat principal + 30 jours après résiliation (données hébergées actives) Données compte client : 5 ans après dernière commande Logs serveur : 3 ans max Rétention résiduelle sauvegardes : voir § 11(3)

Annexe 2 – Mesures techniques et organisationnelles (TOMs)

Les mesures suivantes sont mises en œuvre par LRob afin d'assurer un niveau de protection adapté des données à caractère personnel.

1. Contrôle d'accès physique

Mesure	Mise en œuvre
Accès physique aux serveurs restreint aux datacenters certifiés de l'hébergeur infrastructure (Hetzner)	✓
Hébergement dans des datacenters situés dans l'UE (Allemagne / Finlande)	✓
Surveillance et sécurité physique garanties par Hetzner Online GmbH (ISO 27001, BSI C5 Type 2)	✓

2. Contrôle d'accès électronique

Mesure	Mise en œuvre
Mots de passe complexes générés et stockés via gestionnaire de mots de passe auto-hébergé	✓
Protection anti-bruteforce sur toutes les interfaces d'administration	✓
Accès aux serveurs restreint à LRob et ses intervenants autorisés	✓
Journaux d'accès traçables	✓
Connexions exclusivement via HTTPS/SSL (TLS)	✓
Accès Plesk (éditeur) aux serveurs : uniquement sur demande de support, contrôlé par filtrage IP et clé SSH, temporaire	✓
Mesures supplémentaires côté Client	Responsabilité Client

3. Contrôle d'accès interne

Mesure	Mise en œuvre
Mises à jour et correctifs de sécurité quotidiens automatisés (serveur, site, modules)	✓
Vérification quotidienne des failles de sécurité	✓
Scan d'intégrité quotidien	✓
Pare-feu applicatif (WAF) + pare-feu hardware et software	✓
Bannissement automatique des robots et tentatives d'intrusion (fail2ban, anti-bruteforce)	✓
Accès aux données client restreint au strict nécessaire (principe du moindre privilège)	✓
Maintien et mise à jour des données/logiciels côté Client	Responsabilité Client

4. Sauvegardes

Deux méthodes de sauvegarde complémentaires et indépendantes sont mises en œuvre. Tous les transits sont chiffrés. Les sauvegardes sont chiffrées au repos avec une clé détenue exclusivement par LRob.

Méthode	Périmètre	Destination	Transit	Repos	Rétention
Plesk push	Fichiers, BDD, config Plesk	Storage Box Hetzner Helsinki (FI)	TLS	Clé LRob	3 mois

BackupPC pull	Système complet	NAS LRob Orléans (FR)	SSH	Clé LRob	1 an

Note : les sauvegardes LRob constituent une mesure de résilience technique. Elles ne se substituent pas aux sauvegardes applicatives propres du Client.

5. Contrôle des transferts

Mesure	Mise en œuvre
Chiffrement des données en transit (TLS/HTTPS)	✓
Processus défini de suppression des données actives après résiliation (30 jours)	✓
Restitution des données possible sur demande (fichiers + dump SQL)	✓
Chiffrement des données au repos (données hébergées du Client)	Responsabilité Client

6. Disponibilité, résilience et sécurité réseau

Mesure	Mise en œuvre
Monitoring continu 24h/24, 7j/7	✓
Taux de disponibilité garanti > 99,99 % sur base annuelle	✓
Infrastructure DNS à triple redondance	✓
Protection anti-DDoS (Hetzner)	✓
GTI : 1h en heures ouvrables, 4h hors heures ouvrables	✓
Notification violation de données sous 48h	✓

7. Confidentialité

Mesure	Mise en œuvre
Intervenants LRob soumis à obligation de confidentialité	✓
Partage de données sensibles avec un tiers soumis à accord préalable du Client	✓
Aucune exploitation, cession ou revente des données hébergées	✓
Aucun profilage des utilisateurs, aucune revente de données statistiques	✓
Statistiques auto-hébergées via Matomo (sans transfert vers tiers)	✓

Annexe 3 – Sous-traitants ultérieurs autorisés

LRob fait appel aux sous-traitants ultérieurs suivants pour la fourniture de ses services. Ces sous-traitants traitent des données pour le compte de LRob dans le cadre des services fournis au Client.

Sous-traitant	Adresse	Localisation	Type de service
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Allemagne	UE (DE / FI)	Hébergement serveurs, stockage, réseau, Storage Box (sauvegardes)
Stripe, Inc.	510 Townsend St San Francisco, CA 94103 USA	USA (SCC)	Traitement des paiements
OpenAI / Anthropic	USA	USA (SCC)	Chatbot LRobot (support client)
Intuition Machines (hCaptcha)	USA	USA (SCC)	Protection anti-robot (formulaires contact)
Cloudflare, Inc. (Turnstile)	101 Townsend St San Francisco, CA 94107 USA	USA (SCC)	Protection anti-robot (formulaires contact)

Note : les transferts hors UE (Stripe, OpenAI/Anthropic, hCaptcha, Cloudflare) sont encadrés par des clauses contractuelles types (SCC) conformes à l'art. 46 RGPD. Les données hébergées du Client (serveurs + sauvegardes) restent exclusivement dans l'UE (Allemagne et Finlande).