

DOCUMENT CONTRACTUEL

Accord de Traitement des Données à Caractère Personnel (DPA)

VERSION

2026-09-28

DERNIÈRE MISE À JOUR

28/09/2026

Éditeur

KASAR SAS au capital de 1 000 € · RCS Paris 999 602 865 · 60 rue François 1er, 75008 Paris

Contact

support@kasar.app

Sommaire

1. Définitions	3
2. Rôles et objet	3
3. Durée	3
4. Instructions documentées	4
5. Confidentialité	4
6. Sécurité du traitement (article 32 RGPD)	4
7. Assistance au responsable du traitement	4
8. Notification des violations de données (article 33 RGPD)	5
9. Sous-traitants ultérieurs	5
10. Localisation et transferts hors Union européenne	6
11. Intelligence artificielle	7
12. Sort des données en fin de traitement	8
13. Audit	8
14. Responsabilité	9
15. Articulation avec le Contrat principal	9
Annexe 1 : Description du traitement	9
Annexe 2 : Mesures techniques et organisationnelles de sécurité	10
Annexe 3 : Sous-traitants ultérieurs et services connectés	11

Le présent Accord de Traitement des Données (le « **DPA** ») fait partie intégrante du contrat conclu entre l'Éditeur et le Client (le « **Contrat principal** »), constitué des **Conditions Générales** de KasarCRM ([cgv.md](#)) et, pour la Formule Entreprise, des **Conditions Particulières Entreprise** et du **Bon de commande Entreprise**. Il encadre le traitement, par l'Éditeur pour le compte du Client, des données à caractère personnel contenues dans les Données Client, conformément à l'**article 28 du règlement (UE) 2016/679 (« RGPD »)**.

1. Définitions

Les termes « données à caractère personnel », « traitement », « responsable du traitement », « sous-traitant », « personne concernée », « violation de données » et « sous-traitant ultérieur » ont le sens que leur donne le RGPD. Les termes définis dans le Contrat principal conservent leur sens. Au présent DPA :

- **Responsable du traitement** : le **Client**, qui détermine les finalités et moyens du traitement des Données Client.
- **Sous-traitant** : l'**Éditeur (Kasar)**, qui traite les Données Client pour le compte du Client.
- **Sous-traitant ultérieur** : tout tiers auquel l'Éditeur a recours pour traiter des données pour le compte du Client (annexe 3, section A).
- **Données à Caractère Personnel** : les données à caractère personnel comprises dans les Données Client (annexe 1).

2. Rôles et objet

2.1. Le Client est **responsable du traitement** ; l'Éditeur est **sous-traitant**. Lorsque le Client agit lui-même en qualité de sous-traitant d'un tiers, l'Éditeur est sous-traitant ultérieur, et le Client garantit disposer des autorisations nécessaires de son propre responsable.

2.2. Le présent DPA a pour objet de définir les conditions dans lesquelles l'Éditeur traite les Données à Caractère Personnel pour le compte du Client dans le cadre de la fourniture du Service. La nature, la finalité, la durée, les catégories de données et de personnes concernées sont décrites à l'**annexe 1**.

2.3. Le traitement par l'Éditeur des données dont **il est lui-même responsable** (comptes, facturation, journaux) est exclu du présent DPA et décrit dans la Politique de confidentialité. Le Client donne instruction à l'Éditeur d'établir, à partir des mesures techniques d'utilisation du Service, les statistiques agrégées et anonymisées prévues à l'article 12.3 des Conditions Générales ; ces statistiques ne comprennent aucune donnée relative à des personnes concernées autres que les Utilisateurs.

3. Durée

Le DPA s'applique pendant toute la durée du Contrat principal et tant que l'Éditeur traite des Données à Caractère Personnel pour le compte du Client. Les obligations de confidentialité et de restitution/suppression survivent à son terme.

4. Instructions documentées

- 4.1. L'Éditeur ne traite les Données à Caractère Personnel que sur la base des **instructions documentées** du Client, **y compris s'agissant des transferts vers un pays tiers ou une organisation internationale**. Constituent de telles instructions : le Contrat principal, le présent DPA et ses annexes, et l'usage du Service via ses fonctionnalités (configuration, requêtes, paramètres, activation d'une intégration ou d'une fonctionnalité, automatisations configurées par le Client). Les instructions complémentaires sont adressées par écrit à support@kasar.app ; l'Éditeur y répond dans un délai raisonnable et signale celles qui excéderaient le périmètre du Service ou en modifieraient le coût.
- 4.2. L'Éditeur informe le Client si une instruction lui paraît constituer une violation du RGPD ou d'une autre disposition applicable.
- 4.3. L'Éditeur ne traite les données hors instructions que si le droit de l'Union ou national l'y oblige ; dans ce cas, il en informe le Client avant le traitement, sauf interdiction légale.
- 4.4. **Dépassement d'instructions.** Si l'Éditeur venait à déterminer lui-même les finalités et les moyens d'un traitement, il serait considéré comme responsable de ce traitement (article 28, paragraphe 10, du RGPD). Les parties excluent expressément toute intention en ce sens : hors des traitements visés à l'article 2.3, l'Éditeur n'agit qu'en qualité de sous-traitant.

5. Confidentialité

L'Éditeur veille à ce que les personnes autorisées à traiter les Données à Caractère Personnel, salariés comme prestataires, s'engagent à la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité, et reçoivent la formation nécessaire. Cet engagement survit à la fin de leur contrat de travail ou de prestation.

6. Sécurité du traitement (article 32 RGPD)

- 6.1. L'Éditeur met en œuvre les mesures techniques et organisationnelles appropriées décrites à l'**annexe 2** pour garantir un niveau de sécurité adapté au risque. Ces mesures peuvent évoluer pour tenir compte de l'état de l'art et des risques, **sans réduction du niveau de sécurité global** pendant la durée du Contrat principal.
- 6.2. Ces mesures incluent notamment : l'**isolation logique des données par Organisation** (schéma de base de données dédié par client), le **chiffrement au repos du contenu des communications et des secrets d'accès** aux services tiers (AES-256-GCM), le chiffrement en transit (TLS), le contrôle d'accès et la journalisation.
- 6.3. Le Client reconnaît que, pour fournir les **Fonctionnalités IA** et certaines fonctionnalités d'analyse et de synchronisation, le contenu concerné est **déchiffré** puis traité par l'Éditeur et transmis aux sous-traitants ultérieurs concernés (voir article 11 et annexe 3).

7. Assistance au responsable du traitement

- 7.1. **Droits des personnes.** Compte tenu de la nature du traitement, l'Éditeur aide le Client, par des mesures techniques et organisationnelles appropriées (notamment les fonctionnalités d'accès, d'export, de rectification et de suppression du Service), à répondre aux demandes d'exercice des droits des personnes concernées

(articles 15 à 22 RGPD). Si une demande est adressée directement à l'Éditeur, celui-ci la transmet au Client sans y répondre lui-même, sauf instruction contraire.

7.2. Obligations de sécurité et analyses d'impact. L'Éditeur aide le Client à se conformer à ses obligations au titre des articles 32 à 36 du RGPD (sécurité, notification de violation, analyse d'impact relative à la protection des données, consultation préalable), compte tenu de la nature du traitement et des informations à sa disposition.

7.3. Coût de l'assistance. Sont comprises dans le prix du Service : l'assistance fournie par les fonctionnalités du Service, l'assistance en cas de violation de données (article 8) et la coopération avec une autorité de contrôle qui incombe en propre à l'Éditeur. Toute autre assistance excédant l'usage normal du Service et ce qu'exige raisonnablement l'article 28 du RGPD (notamment les extractions sur mesure, les réponses à des questionnaires spécifiques ou la contribution détaillée à une analyse d'impact au-delà d'une (1) journée de travail) fait l'objet d'un devis préalable accepté par le Client, établi au tarif journalier en vigueur de l'Éditeur. Rien n'est dû lorsque la demande trouve son origine dans un manquement de l'Éditeur.

8. Notification des violations de données (article 33 RGPD)

L'Éditeur notifie au Client toute violation de Données à Caractère Personnel **dans les meilleurs délais**, et dans la mesure du possible dans les **quarante-huit (48) heures** suivant le moment où il a acquis une certitude raisonnable qu'une violation affectant les Données du Client s'est produite, afin de permettre au Client de respecter le délai de l'article 33 du RGPD. Lorsque la violation affecte un sous-traitant ultérieur, ce délai court à compter de l'information de l'Éditeur par celui-ci. La notification est adressée par message à l'adresse de contact de l'Administrateur et, lorsqu'il est renseigné, au contact sécurité du Client.

La notification décrit, dans la mesure des informations disponibles : la **nature** de la violation et, si possible, les catégories et le nombre approximatif de personnes concernées et d'enregistrements ; les **conséquences probables** ; les **mesures** prises ou proposées pour y remédier et en atténuer les effets ; les **coordonnées** du point de contact de l'Éditeur. Lorsque toutes ces informations ne sont pas disponibles dans ce délai, l'Éditeur adresse une première notification partielle, puis communique les informations manquantes au fur et à mesure, dans les meilleurs délais.

L'Éditeur ne procède à aucune notification à l'autorité de contrôle ou aux personnes concernées au nom du Client, sauf instruction écrite de celui-ci. La notification d'une violation ne vaut pas reconnaissance d'une faute ou d'une responsabilité de l'Éditeur.

9. Sous-traitants ultérieurs

9.1. Autorisation générale. Le Client **autorise** l'Éditeur à recourir aux sous-traitants ultérieurs listés à la **section A de l'annexe 3** pour les besoins du Service.

9.2. Garanties. L'Éditeur impose à chaque sous-traitant ultérieur, par contrat, les obligations de protection des données prévues à l'article 28, paragraphe 4, du RGPD, offrant un niveau de protection substantiellement équivalent à celui du présent DPA compte tenu de la nature du service fourni, en particulier l'obligation de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Lorsque le sous-traitant ultérieur ne propose que ses conditions standard, l'Éditeur s'assure qu'elles comportent ces obligations. L'Éditeur demeure responsable envers le Client de l'exécution par ces sous-traitants de leurs obligations, dans les conditions et limites de l'article 14.

9.3. **Changements.** L'Éditeur informe le Client de tout projet d'ajout ou de remplacement de sous-traitant ultérieur au moins **trente (30) jours** avant, par tout moyen approprié (mise à jour de l'annexe 3 et notification). Le Client peut s'opposer, par écrit et pour un motif objectif tenant à la protection des données, dans un délai de **quatorze (14) jours**. L'Éditeur s'efforce alors de proposer une solution, notamment la désactivation de la fonctionnalité concernée pour l'Organisation du Client ; à défaut de solution dans les trente (30) jours de l'opposition, le Client peut résilier, sans pénalité, la partie du Service qui recourt au sous-traitant ultérieur concerné ou, si elle n'est pas dissociable, l'Abonnement, avec effet à la date de mise en œuvre de ce sous-traitant ultérieur. Seules les sommes payées d'avance au titre de la partie résiliée et de la période non courue sont remboursées. Une opposition non fondée sur un motif objectif tenant à la protection des données est sans effet.

9.4. **Urgence.** En cas d'urgence tenant à la sécurité ou à la défaillance d'un sous-traitant ultérieur, l'Éditeur peut procéder à son remplacement sans respecter le délai de l'article 9.3 ; il en informe le Client sans délai, et celui-ci dispose alors du droit d'opposition prévu à cet article.

10. Localisation et transferts hors Union européenne

10.1. **Localisation.** L'hébergement principal des Données à Caractère Personnel (base de données et stockage de fichiers) est situé dans l'**Union européenne** (Irlande) ; les fonctions applicatives s'exécutent dans l'Union européenne (France). Certains traitements sont toutefois réalisés **hors de l'Union européenne**, en particulier aux **États-Unis** :

- l'infrastructure de synchronisation et de traitement asynchrone (emails, messages LinkedIn et WhatsApp, imports, automatisations) et le robot d'enregistrement de réunions, exploités sur un cluster **DigitalOcean** situé à **New York** ;
- l'acheminement des appels de la téléphonie native par **Twilio** (article 10.4) ;
- certaines Fonctionnalités IA (article 11).

La liste des traitements concernés, leur localisation et le mécanisme de transfert applicable figurent à l'annexe 3. **La migration du cluster DigitalOcean vers une région de l'Union européenne est prévue** ; l'annexe 3 sera mise à jour lorsqu'elle sera effective.

10.2. **Mécanismes de transfert.** Tout transfert hors EEE est encadré par un mécanisme conforme au chapitre V du RGPD : décision d'adéquation, y compris le **cadre de protection des données UE-États-Unis** (« **DPF** ») pour les destinataires certifiés, ou **clauses contractuelles types** de la Commission européenne (décision d'exécution (UE) 2021/914). Lorsque l'Éditeur transfère lui-même des données à un sous-traitant ultérieur établi hors EEE et non certifié, il agit comme **exportateur** et conclut les clauses contractuelles types applicables (**module 3**, sous-traitant vers sous-traitant ultérieur). Lorsque le cocontractant de l'Éditeur est établi dans l'Union et transfère lui-même les données hors EEE, ce transfert est encadré par les garanties que ce cocontractant met en place, telles qu'indiquées à l'annexe 3.

10.3. **Mesures supplémentaires et analyses d'impact des transferts.** L'Éditeur met en œuvre les mesures supplémentaires recommandées par le CEPD (recommandations 01/2020) lorsqu'elles sont pertinentes : chiffrement en transit, minimisation des données transmises, engagements contractuels de non-conservation lorsqu'ils sont disponibles. L'Éditeur établit et tient à jour une analyse d'impact pour chaque transfert fondé sur des clauses contractuelles types dont il est l'exportateur. Une synthèse est communiquée au Client sur demande écrite, sous obligation de confidentialité, dans un délai raisonnable.

10.4. **Téléphonie native.** Les appels de la téléphonie native (« kasar-voip ») passés depuis l'application sont acheminés et traités par **Twilio aux États-Unis** (région us1). Les enregistrements sont stockés dans l'Union européenne (annexe 3). Ce transfert est encadré par des clauses contractuelles types (article 10.2).

10.5. **Demandes d'autorités de pays tiers.** Si l'Éditeur reçoit d'une autorité publique d'un pays tiers une demande d'accès aux Données à Caractère Personnel, il en informe le Client sans délai, sauf interdiction légale ; il évalue la légalité de la demande au regard du droit de l'Union, la conteste lorsqu'elle lui paraît manifestement illégale, ne communique que le minimum requis et documente la demande. L'Éditeur ne peut répondre des demandes adressées directement à ses sous-traitants ultérieurs, qui sont tenus à leur égard par les garanties visées à l'article 10.2.

11. Intelligence artificielle

11.1. Les Fonctionnalités IA recourent à des fournisseurs de modèles d'IA tiers, agissant en qualité de sous-traitants ultérieurs (annexe 3), auxquels le contenu concerné est transmis déchiffré. Les fournisseurs, leurs fonctions et leurs lieux de traitement sont décrits à l'article 13.2 des Conditions Générales et à l'annexe 3.

11.2. **Entraînement des modèles.** Conformément à l'article 13.3 des Conditions Générales :

- l'Éditeur **n'utilise pas** les Données à Caractère Personnel pour entraîner ou améliorer des modèles d'intelligence artificielle ;
- **Anthropic** est tenue, par son contrat avec l'Éditeur, de ne pas utiliser le contenu transmis pour entraîner ses modèles ; **OpenAI** ne l'utilise pas à cette fin selon les conditions applicables à son interface de programmation ;
- **Deepgram** ne l'utilise pas pour entraîner ou améliorer ses modèles, l'Éditeur ayant exclu le contenu transmis de son programme d'amélioration des modèles.

11.3. **Conservation par les fournisseurs d'IA.**

- **Anthropic Ireland, Ltd** : l'Éditeur a souscrit un engagement contractuel de **non-conservation** (« zero retention ») : le contenu transmis est traité pour produire le résultat destiné au Client puis n'est pas conservé par Anthropic, sauf obligation légale ou lutte contre un usage contraire à sa politique d'utilisation ; il n'est pas utilisé pour entraîner ses modèles.
- **OpenAI** : selon la documentation d'OpenAI, les journaux de surveillance des abus des interfaces de synthèse et de transcription vocales sont conservés **trente (30) jours** par défaut.
- **Deepgram, Inc.** : Deepgram peut conserver temporairement le contenu transmis, selon les conditions de son interface de programmation, notamment à des fins de sécurité ; il ne l'utilise pas pour entraîner ses modèles (article 11.2).

11.4. **Décisions automatisées et règlement sur l'IA.** L'Éditeur ne prend aucune décision fondée exclusivement sur un traitement automatisé au sens de l'article 22 du RGPD. Les automatisations, campagnes et actions de Léo sont configurées et déclenchées par le Client, qui en répond (articles 13.7 et 13.8 des Conditions Générales). Les pratiques interdites par l'article 5 du règlement (UE) 2024/1689 sont prohibées.

12. Sort des données en fin de traitement

- 12.1. **Restitution.** À la fin du Contrat principal, le Client dispose de la période de récupération prévue à l'article 17.6 des Conditions Générales, d'au moins **trente (30) jours**, pour exporter ses Données à Caractère Personnel en formats ouverts et lisibles par machine, dans les conditions des articles 17.1 et 17.11 des Conditions Générales.
- 12.2. **Suppression.** À l'expiration de cette période, l'Éditeur **supprime** les Données à Caractère Personnel de ses environnements de production et demande leur suppression à ses sous-traitants ultérieurs dans les conditions de leurs contrats, sous réserve des sauvegardes (article 12.3) et des obligations légales de conservation ; l'Éditeur indique alors au Client, sur demande, la disposition qui l'y contraint et la durée concernée. Le Client peut demander une suppression anticipée par écrit.
- 12.3. **Sauvegardes.** Les copies résiduelles contenues dans les sauvegardes ne sont pas supprimées individuellement : elles sont effacées au fil du cycle de rotation des sauvegardes de l'hébergeur, l'Éditeur ayant pour objectif leur disparition dans les meilleurs délais. Jusqu'à leur effacement, elles restent protégées par les mesures de l'annexe 2, ne font l'objet d'aucun traitement actif et ne sont utilisées qu'aux fins de restauration (article 15.6 des Conditions Générales). En cas de restauration, l'Éditeur réapplique les suppressions intervenues depuis la sauvegarde.
- 12.4. **Confirmation.** L'Éditeur délivre une **confirmation écrite de la suppression** sur demande du Client.

13. Audit

- 13.1. **Information.** L'Éditeur met à la disposition du Client les informations nécessaires pour démontrer le respect de l'article 28 du RGPD : le présent DPA et ses annexes, le registre visé à l'article 13.5 et, sur demande, les réponses à un questionnaire de sécurité raisonnable, une fois par période de douze (12) mois.
- 13.2. **Audit documentaire par défaut.** Tout audit est d'abord conduit sur pièces, à partir des informations visées à l'article 13.1.
- 13.3. **Audit sur place.** Lorsque le Client estime, à l'issue de l'audit documentaire, que les informations fournies ne suffisent pas à démontrer le respect de l'article 28 du RGPD, il peut réaliser un audit sur place, ou le faire réaliser par un auditeur indépendant qui n'est pas un Concurrent de l'Éditeur et qui est tenu à la confidentialité, dans les conditions suivantes :
- au plus **une fois par période de douze (12) mois** ;
 - moyennant un préavis écrit d'au moins **trente (30) jours** et un plan d'audit communiqué au moins quinze (15) jours avant ;
 - pendant les Heures Ouvrées (de 9 h à 18 h, heure de Paris, les Jours Ouvrés), pour une durée de **deux (2) Jours Ouvrés** au plus, sans perturber les opérations de l'Éditeur ni accéder aux données d'autres clients ou aux secrets d'affaires de l'Éditeur, lesquels sont consultés sur place, sans copie ;
 - **aux frais du Client**, qui supporte ses propres coûts et ceux de son auditeur ainsi que le temps passé par l'Éditeur, au tarif journalier communiqué avant l'audit ;
 - le rapport d'audit est remis gratuitement à l'Éditeur.

L'audit porte sur l'Éditeur et s'exerce en priorité à distance. Il ne s'étend pas aux sous-traitants ultérieurs, dont la conformité est démontrée par leurs certifications et rapports d'audit (notamment SOC 2, ISO 27001), que l'Éditeur communique lorsqu'il en dispose.

13.4. **Exceptions.** Le préavis est réduit à **dix (10) Jours Ouvrés**, et la périodicité et la prise en charge du temps de l'Éditeur ne s'appliquent pas, lorsque l'audit fait suite à une **violation de données avérée** affectant les Données du Client ou à la **demande d'une autorité de contrôle**. Lorsqu'un audit établit un manquement de l'Éditeur à ses obligations au titre de l'article 28 du RGPD, l'Éditeur ne facture pas son temps et remédie au manquement à ses frais selon un plan d'action convenu ; chaque partie conserve la charge de ses autres frais. Le coût de la remise en conformité, qui relève des obligations propres de l'Éditeur, ne s'impute pas sur le plafond visé à l'article 14.

13.5. **Registre et point de contact.** L'Éditeur tient le registre des catégories d'activités de traitement effectuées pour le compte du Client (article 30, paragraphe 2, du RGPD) et le communique sur demande. Le point de contact de l'Éditeur pour toute question relative à la protection des données, y compris le signalement des incidents de sécurité et des violations présumées, est support@kasar.app.

14. Responsabilité

14.1. La responsabilité de l'Éditeur au titre du présent DPA, y compris au titre des données à caractère personnel, est soumise aux stipulations de l'**article 16 des Conditions Générales**, et notamment au **plafond unique** de son article 16.2 : les sommes effectivement payées par le Client au cours des douze (12) mois précédant le fait générateur, avec un minimum de cent euros (100 €), sans jamais excéder **cinquante mille euros (50 000 €)**, quelle que soit la Formule. Le présent DPA n'institue **aucun plafond distinct ni majoré** ; les sommes dues au titre du DPA et au titre du Contrat principal s'imputent sur ce même plafond.

14.2. Ce plafond ne s'applique pas en cas de faute lourde, de dol ou de dommage corporel (article 16.3 des Conditions Générales). Il régit les relations entre les parties, y compris l'action récursoire exercée entre elles au titre de l'article 82, paragraphe 5, du RGPD ; il ne limite pas les droits que les personnes concernées tiennent de l'article 82 du RGPD à l'égard de chacune des parties.

15. Articulation avec le Contrat principal

15.1. Pour ce qui relève de l'**article 28 du RGPD**, les stipulations du présent DPA s'appliquent en toute hypothèse et priment sur toute stipulation contraire du Contrat principal (article 2.3 des Conditions Générales). Pour le reste, l'ordre de priorité est celui de l'article 2.2 des Conditions Générales.

15.2. Le droit applicable et la juridiction sont ceux du Contrat principal.

Annexe 1 : Description du traitement

Élément	Description
Responsable du traitement	Le Client (l'Organisation)
Sous-traitant	KASAR (KasarCRM), SAS, RCS Paris 999 602 865, 60 rue François 1er, 75008 Paris
Objet	Fourniture d'un service de CRM en mode SaaS et de ses fonctionnalités associées
Nature des opérations	Collecte, enregistrement, organisation, structuration, conservation, consultation, analyse (y compris par IA), synchronisation, transmission, export, suppression

Élément	Description
Finalités	Permettre au Client de gérer sa relation client : contacts, entreprises, opportunités, communications (email, LinkedIn, WhatsApp, téléphonie), réunions, tâches, notes, tableaux de bord
Durée	Durée du Contrat principal + délais de restitution/suppression (article 12)

Catégories de personnes concernées (déterminées par le Client) :

- Les contacts et correspondants du Client (clients, prospects, partenaires) ;
- Les Utilisateurs et membres de l'équipe du Client ;
- Toute personne mentionnée dans les communications ou enregistrements synchronisés.

Catégories de Données à Caractère Personnel (déterminées par le Client) :

- Données d'identification et de contact : nom, prénom, adresses email, numéros de téléphone, adresse postale, URL LinkedIn, photo, fonction ;
- Contenu des **communications synchronisées** : emails (objet, corps, participants), messages LinkedIn et WhatsApp, métadonnées d'appels téléphoniques ;
- **Enregistrements et transcriptions** d'appels et de réunions (si activés par le Client) ;
- Données relationnelles et commerciales : notes, tâches, statut, source, historique d'interactions, données d'enrichissement, résumés générés par IA ;
- Toute autre donnée que le Client choisit de saisir ou d'importer dans des champs libres.

Le Client s'interdit d'importer, de saisir ou d'organiser la collecte de **catégories particulières de données** (article 9 RGPD), sous réserve de leur présence incidente, dans les conditions de l'article 11.4 des Conditions Générales.

Annexe 2 : Mesures techniques et organisationnelles de sécurité

- **Isolation des données** : un schéma de base de données PostgreSQL dédié par Organisation, avec isolation logique au niveau de chaque transaction ; validation stricte des identifiants de schéma.
- **Chiffrement au repos** : chiffrement AES-256-GCM du contenu des communications (corps des messages) et des secrets/identifiants tiers (jetons OAuth, sessions).
- **Chiffrement en transit** : TLS pour les communications entre les Utilisateurs et le Service et avec les sous-traitants ultérieurs ; politique de sécurité de contenu (CSP) restrictive.
- **Contrôle d'accès** : authentification des Utilisateurs, comptes nominatifs, gestion des rôles et habilitations par l'Administrateur.
- **Cloisonnement des secrets** : les données de carte de paiement ne transitent jamais par l'Éditeur (collecte directe navigateur → prestataire de paiement) ; les jetons d'accès tiers sont chiffrés.
- **Journalisation et supervision** : journalisation des opérations sur les enregistrements, des imports, des intégrations et des connexions ; supervision applicative.
- **Sauvegardes** : sauvegardes gérées par l'hébergeur de base de données.
- **Sous-traitance** : engagements contractuels imposés aux sous-traitants ultérieurs (article 9.2).

Cette annexe décrit l'état des mesures à la date de la dernière mise à jour ; elle peut évoluer, sans réduction du niveau de sécurité global.

Annexe 3 : Sous-traitants ultérieurs et services connectés

Dernière mise à jour : 28/09/2026. Toute modification est notifiée dans les conditions de l'article 9.3.

A. Sous-traitants ultérieurs de l'Éditeur

Ils interviennent pour toutes les Organisations, dès que la fonctionnalité concernée est utilisée, sans autre action du Client.

Sous-traitant	Finalité	Localisation du traitement	Transfert hors EEE et garanties
Supabase	Base de données PostgreSQL, stockage de fichiers	Irlande (AWS eu-west-1)	Sans objet
Vercel	Exécution de l'application, supervision	France (région cdg1)	Sans objet
Upstash / Redis	Cache, files de traitement, présence	Région indiquée dans les conditions d'Upstash	Possible. Clauses contractuelles types (DPA d'Upstash)
Amazon Web Services (S3)	Stockage des enregistrements de réunions et d'appels	Irlande (eu-west-1)	Sans objet
DigitalOcean, LLC	Cluster hébergeant les workers de synchronisation et de traitement (emails, messages LinkedIn et WhatsApp, imports, automatisations), la passerelle WhatsApp et le robot d'enregistrement de réunions. Contenu des communications et sessions d'accès traités sur ce cluster	États-Unis (New York, région nyc1). Migration vers une région de l'Union européenne prévue	Oui. Clauses contractuelles types (module 3) prévues par le DPA de DigitalOcean
Anthropic Ireland, Ltd	Modèles d'IA : génération de texte, analyse, résumé, assistant Léo, recherche web. Engagement contractuel de non-conservation (« zero retention », article 11.3) ; pas d'entraînement	Cocontractant établi en Irlande. Selon Anthropic, l'inférence peut être acheminée par défaut vers des serveurs situés aux États-Unis, en Europe, en Asie ou en Australie	Possible. Transferts hors EEE effectués par Anthropic sous clauses contractuelles types (DPA d'Anthropic)
Deepgram, Inc.	Transcription audio des réunions, des appels et des mémos vocaux. Pas d'entraînement (article 11.2) ; conservation temporaire selon les conditions de son API	États-Unis	Oui. Clauses contractuelles types (module 3)

Sous-traitant	Finalité	Localisation du traitement	Transfert hors EEE et garanties
OpenAI	Synthèse vocale des réponses de Léo sur l'application mobile ; transcription de secours (Whisper) lorsque la transcription principale est indisponible. Pas d'entraînement selon les conditions de l'API ; journaux de surveillance des abus conservés 30 jours	États-Unis	Oui. Cocontractant et garanties selon le DPA d'OpenAI ; transferts sous clauses contractuelles types
Twilio	Téléphonie native « kasar-voip » : acheminement des appels, numéros, enregistrements (article 10.4)	États-Unis (acheminement des appels) ; Irlande (stockage des enregistrements)	Oui. Clauses contractuelles types
Dropcontact	Recherche et vérification d'adresses email professionnelles, lors de l'enrichissement et de la recherche de prospects	France (UE)	Sans objet
Stripe	Paiements et facturation	UE / États-Unis	Clauses contractuelles types
Resend	Emails transactionnels (invitations, liens de connexion)	États-Unis	Clauses contractuelles types

B. Services tiers connectés à l'initiative du Client

Ces services ne traitent de données que si le Client **connecte l'intégration correspondante**, et pour le seul périmètre qu'il autorise. Le Client les choisit, entretient sa propre relation contractuelle avec chacun d'eux et en accepte les conditions : ils agissent pour le compte du Client, ou en qualité de responsables de traitement indépendants, et **ne sont pas des sous-traitants ultérieurs de l'Éditeur**. L'Éditeur n'y accède que pour exécuter l'intégration, sur instruction du Client ; il ne répond pas de leurs traitements, et les articles 9 et 10 ne leur sont pas applicables. Le traitement que l'Éditeur réalise lui-même sur les données issues de ces services relève en revanche de la section A (notamment DigitalOcean pour la synchronisation). La liste ci-dessous est fournie à titre d'information ; la localisation et les garanties de chaque service relèvent de ses propres conditions.

Service	Famille	Données concernées
Google (Gmail, Calendar, Meet)	Messagerie, agenda, transcripts	Emails, événements, transcripts de réunions
Microsoft 365 (Graph)	Messagerie, agenda	Emails, événements
LinkedIn	Messagerie (connecteur de l'article 10.6 des Conditions Générales)	Messages et conversations LinkedIn du compte connecté
WhatsApp	Messagerie (connecteur de l'article 10.6 des Conditions Générales)	Messages WhatsApp du compte connecté
Meta Lead Ads	Publicité	Prospects issus des formulaires de génération de leads
Slack	Connecteur de données	Messages des canaux auxquels le Client donne accès

Service	Famille	Données concernées
Notion, Airtable, Google Sheets	Connecteurs de données	Contenus des bases et feuilles connectées
Supabase / PostgreSQL du Client	Source de données	Contenus des tables connectées
Fathom, Granola	Comptes rendus de réunions	Enregistrements, transcriptions et notes de réunions
Aircall	Téléphonie	Appels, enregistrements et transcriptions
Applications connectées par le Client (API, serveur MCP, webhooks)	Article 10.8 des Conditions Générales	Données que le Client choisit de leur transmettre