

CONVENTION DE TRAITEMENT DES DONNÉES

(Data Processing Agreement — DPA)

Annexe au Contrat de Mandat

CaRa Global Suisse Sàrl

c/o Fiduciaire CM Fidatel SA — Place du Forum 2, 1073 Savigny / VD, Suisse

CHE-115.612.632

cara-global.ch

Version 1.6 — 27 août 2026

Parties

Le Mandant (« Responsable du traitement »)

Le Mandant est la personne morale ou physique qui souscrit une ou plusieurs Assistantes. Il est identifié par les informations qu'il fournit lors de la souscription (raison sociale, adresse de facturation, adresse électronique et, le cas échéant, numéro IDE), telles qu'enregistrées par le prestataire de paiement et reprises dans le courriel de confirmation.

Le Mandataire (« Sous-traitant »)

CaRa Global Suisse Sàrl

IDE : CHE-115.612.632

Siège : c/o Fiduciaire CM Fidatel SA — Place du Forum 2, 1073 Savigny / VD, Suisse

Représentée par : Carine Rasconi, Gérante-associée unique

Contact protection des données : carine@cara-global.ch

1. Préambule et objet

La présente Convention de Traitement des Données (ci-après « DPA ») complète le Contrat de Mandat conclu entre le Mandant et le Mandataire. Elle définit les conditions dans lesquelles le Mandataire traite, pour le compte du Mandant, des données à caractère personnel dans le cadre des Assistantes contractuellement souscrites.

Le présent DPA s'inscrit dans le respect :

- De la Loi fédérale sur la protection des données (LPD) suisse révisée, en vigueur depuis le 1er septembre 2023, et de son ordonnance d'exécution (OPDo).
- Du Règlement (UE) 2016/679 (RGPD) lorsque celui-ci est applicable au traitement, notamment en présence de personnes concernées résidant dans l'Union européenne.
- Des recommandations du Préposé fédéral à la protection des données et à la transparence (PFPDT).

En cas de divergence entre le Contrat de Mandat et le présent DPA, ce dernier prévaut sur les questions relatives à la protection des données.

2. Définitions

Données personnelles : toute information se rapportant à une personne physique identifiée ou identifiable au sens de la LPD et du RGPD.

Traitement : toute opération relative à des données personnelles, notamment la collecte, l'enregistrement, la conservation, la modification, la transmission, la suppression ou la destruction.

Responsable du traitement : le Mandant, qui détermine les finalités et les moyens du traitement.

Sous-traitant : le Mandataire (CaRa Global Suisse Sàrl), qui traite les données pour le compte du Responsable du traitement.

Sous-traitant ultérieur : tiers auquel le Mandataire confie une partie du traitement (ex. hébergeur, prestataire SaaS).

Violation de données : tout incident de sécurité entraînant la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données personnelles.

Assistantes : désigne collectivement les prestations CaRa Admin System, comprenant notamment les Assistantes contractuellement souscrites par le Mandant, accessibles via l'application « CaRa dans la poche », ainsi que l'Audit Stratégique. Toute référence ultérieure aux « Assistantes » dans le présent DPA renvoie à cette définition.

3. Nature et finalité du traitement

Le Mandataire traite les données personnelles aux seules fins suivantes, en lien avec les Assistantes contractuellement souscrites :

1. Saisie automatisée de pièces comptables (Assistante Créanciers) : extraction des données de factures fournisseurs au moyen d'un modèle d'intelligence artificielle, classement et archivage structuré.
2. Diagnostic stratégique et restitution d'audit (Audit Stratégique) : collecte de réponses au questionnaire, génération du rapport personnalisé, envoi par courrier électronique.
3. Communication transactionnelle : envoi d'emails d'onboarding, de confirmation, de relance et de support technique.
4. Gestion de l'abonnement et facturation : encaissement via prestataire de paiement, émission de factures.
5. **Point de tenue trimestriel** (Assistances CaRa, dès deux Assistances actives) : consultation, par une personne autorisée du Mandataire, des données déjà traitées pour le compte du Mandant, aux seules fins d'établir un point de tenue écrit et signé qui lui est remis. Cette consultation s'effectue en lecture seule et n'emporte aucune modification des données du Mandant.
6. **Relances de créances pour le compte du Mandant** (Assistance Encaissement) : traitement des données relatives aux clients et débiteurs du Mandant — identité, coordonnées, montants, échéances et références des factures — aux fins de rédiger un rappel de paiement, de le soumettre à la validation préalable du Mandant, puis de l'expédier au nom et pour le compte de celui-ci. Le Mandataire agit sur mandat (art. 394 CO) ; il n'acquiert aucune créance, n'agit jamais en son propre nom et n'encaisse aucun fonds.

Le Mandataire s'engage à ne pas traiter les données pour des finalités autres que celles décrites ci-dessus, sans instruction écrite préalable du Mandant.

Accès humain en lecture seule

Le Mandant est informé qu'une personne autorisée du Mandataire peut accéder en lecture seule aux données traitées pour son compte, aux seules finalités énumérées au présent article — notamment l'établissement du point de tenue trimestriel et le support technique. Cet accès est nominatif, limité aux personnes autorisées, journalisé, et ne permet aucune modification des données du Mandant. Aucun accès humain n'a lieu à d'autres fins que celles énumérées ci-dessus.

3 bis. Instructions du Mandant

Le Mandataire traite les données personnelles uniquement sur la base des instructions documentées du Mandant, telles qu'établies par le Contrat de Mandat, le présent DPA et toute instruction écrite ultérieure, sauf obligation légale ou réglementaire contraire à laquelle le Mandataire serait soumis.

Si le Mandataire estime qu'une instruction du Mandant viole la LPD, le RGPD ou tout autre droit applicable, il en informe immédiatement le Mandant et peut suspendre l'exécution de l'instruction concernée jusqu'à clarification.

4. Catégories de données traitées

Selon les Assistantes contractées, les catégories de données suivantes peuvent être traitées :

- Données d'identification : raison sociale, nom, prénom, fonction.
- Données de contact : adresse postale, adresse électronique, numéro de téléphone.
- Données comptables et financières : factures fournisseurs (montants, dates, références), références bancaires figurant sur les pièces, identifiants de paiement Stripe (sans données de carte de paiement).
- Données techniques : journaux d'utilisation de l'application, jetons de session, journaux d'orchestration et d'accès.
- Données contenues dans les pièces téléversées : toute information personnelle figurant sur les factures fournisseurs ou justificatifs transmis par le Mandant (notamment données concernant des tiers fournisseurs).
- **Données relatives aux clients et débiteurs du Mandant** : identité, coordonnées, montants, échéances, références et état de paiement des factures émises par le Mandant, ainsi que le contenu des rappels adressés en son nom (brique « Débiteurs & relances » de l'Assistante Encaissement, lorsqu'elle est activée).

Catégories de personnes concernées

- Représentants légaux et collaborateurs du Mandant.
- Tiers identifiables dans les pièces comptables téléversées (fournisseurs, prestataires, intervenants).
- Clients et débiteurs du Mandant, lorsque celui-ci a activé la brique « Débiteurs & relances ».

5. Durée du traitement et conservation des données

Pendant la durée du Contrat de Mandat

L'ensemble des données traitées est conservé pour les besoins de l'exécution des Assistantes. Aucune suppression périodique automatique ne s'applique tant que le Contrat est actif.

Après la résiliation ou l'expiration du Contrat

Le Mandataire conserve les données pour une durée maximale de douze (12) mois supplémentaires, à seule fin de protection contre d'éventuels litiges. Au terme de cette période post-contrat, l'ensemble des données est supprimé de manière définitive et irréversible chez le Mandataire et auprès de ses sous-traitants ultérieurs, sous réserve d'obligations légales contraires.

Archivage légal

Le Mandant demeure seul responsable de l'archivage légal de ses pièces comptables conformément aux articles 957 et 958f du Code des Obligations suisse (durée de conservation minimale de dix ans). Le Mandataire ne se substitue pas à cette obligation, sauf souscription explicite à un service d'archivage longue durée séparé.

6. Sous-traitants ultérieurs autorisés

Le Mandataire informe le Mandant qu'il recourt aux sous-traitants ultérieurs listés ci-dessous pour assurer la prestation. Le Mandant donne son accord exprès à cette liste par la signature du présent DPA.

Sous-traitant	Pays	Finalité	Garanties / Cadre
Infomaniak Network SA	Suisse (Genève)	Hébergement de l'ensemble de l'infrastructure : kDrive (archivage des pièces comptables PDF), serveurs virtuels (application, base de données, orchestration des traitements, extraction automatisée) et messagerie professionnelle.	LPD CH ; ISO 27001 ; souveraineté suisse
Mistral AI	France (UE)	Lecture automatisée des pièces PDF (extraction des données de facture) — traitement éphémère, sans rétention ni réutilisation pour entraînement. Assistantes Créanciers et Débiteurs.	RGPD natif ; pas de réutilisation des données pour entraînement
Stripe Payments Europe Ltd.	Irlande (UE)	Encaissement des abonnements et des paiements uniques. Toutes les Assistantes.	RGPD ; PCI-DSS niveau 1
ElevenLabs Inc.	États-Unis	Synthèse et compréhension vocale de l'agent d'accueil téléphonique. Assistante Réceptionniste uniquement.	Clauses contractuelles types UE ; choix exprès du Mandant
Twilio Inc.	États-Unis	Téléphonie de l'agent d'accueil : ligne fixe suisse et numéro international pour les SMS. Assistante	Clauses contractuelles types UE ; choix exprès du Mandant

		Réceptionniste uniquement.	
--	--	----------------------------	--

Modification de la liste

Toute adjonction ou substitution d'un sous-traitant ultérieur fait l'objet d'une notification écrite préalable au Mandant (par courriel) avec un préavis minimum de trente (30) jours. Le Mandant dispose de ce délai pour formuler une objection motivée. À défaut d'objection, la modification est réputée acceptée.

Version 1.6 (27 août 2026) : la présente version n'introduit aucun sous-traitant ultérieur nouveau. Le préavis de trente (30) jours prévu ci-dessus ne s'applique donc pas. Les finalités ajoutées à l'article 3 sont exécutées sur l'infrastructure Infomaniak déjà listée (hébergement suisse et messagerie professionnelle) ; l'expédition des rappels au nom du Mandant emprunte cette même messagerie.

7. Localisation des données et transferts internationaux

Données primaires

L'ensemble des données du Mandant — pièces comptables, base de données et traitements — est stocké et traité en Suisse, sur l'infrastructure Infomaniak (kDrive et serveurs virtuels, datacenter de Genève).

Métadonnées et logs

Pour les Assistantes administratives (Créanciers, Débiteurs, Rapprochement bancaire), les seuls traitements hors de Suisse ont lieu au sein de l'Union européenne : lecture des pièces (Mistral AI, France) et encaissement (Stripe, Irlande). L'Assistante Réceptionniste, souscrite séparément, fait intervenir des prestataires établis aux États-Unis (Twilio, ElevenLabs) pour la téléphonie et la voix.

Garanties pour les transferts hors Suisse / UE

Pour les transferts vers des pays ne disposant pas d'une décision d'adéquation au sens de la LPD ou du RGPD, le Mandataire s'appuie sur :

- Les Clauses Contractuelles Types adoptées par la Commission européenne (décision 2021/914).
- Le cadre EU-US Data Privacy Framework (lorsque le sous-traitant y est inscrit).
- Des engagements contractuels équivalents avec chaque sous-traitant.

8. Mesures de sécurité

Le Mandataire met en œuvre les mesures techniques et organisationnelles appropriées, notamment :

- Chiffrement des communications en transit (TLS 1.2 minimum, TLS 1.3 recommandé).
- Chiffrement au repos sur les principales infrastructures (kDrive, base de données, Stripe).
- Authentification à deux facteurs sur l'ensemble des comptes administrateurs.
- Accès aux données limité aux personnes autorisées et tracé.

- Accès humain en lecture seule uniquement, nominatif et journalisé (cf. art. 3, « Accès humain en lecture seule »).
- Sauvegardes automatiques et historisation (kDrive : versions conservées 30 jours).
- Cloisonnement strict entre les environnements de test et de production.
- Revue annuelle des sous-traitants et de leurs garanties.
- Formation continue du personnel à la protection des données.

9. Droits des personnes concernées

Le Mandant reste l'interlocuteur principal des personnes concernées pour l'exercice de leurs droits. Le Mandataire l'assiste dans le traitement des demandes, dans la mesure de ses possibilités techniques.

Sont notamment garantis les droits suivants :

- Droit d'accès et d'information.
- Droit de rectification.
- Droit à l'effacement (« droit à l'oubli »).
- Droit à la portabilité des données.
- Droit d'opposition et de limitation du traitement.

Le Mandataire répond aux sollicitations du Mandant dans un délai de quinze (15) jours ouvrables.

Contact dédié protection des données : **carine@cara-global.ch** (Carine Rasconi, Gérante-associée unique).

10. Notification des violations de données

En cas de violation de données affectant les données personnelles traitées pour le compte du Mandant, le Mandataire :

7. Notifie le Mandant dans les meilleurs délais et au plus tard soixante-douze (72) heures après en avoir pris connaissance.
8. Documente la nature de la violation, les catégories de données concernées, les conséquences probables et les mesures prises ou envisagées.
9. Coopère pleinement avec le Mandant pour les notifications éventuelles à l'autorité de contrôle compétente (PFPDT en Suisse, autorités RGPD le cas échéant) et aux personnes concernées.
10. Tient un registre interne de tous les incidents de sécurité significatifs.

11. Sort des données à la fin du contrat

À l'expiration ou à la résiliation du Contrat de Mandat, et sur instruction écrite du Mandant :

11. Le Mandataire cesse immédiatement tout traitement actif des données.
12. Le Mandataire restitue au Mandant l'ensemble des données dans un format structuré et exploitable (export tableur et archive documentaire).

13. Au terme de la période de conservation prévue à l'article 5 (12 mois), les données sont supprimées de manière définitive chez le Mandataire et auprès des sous-traitants ultérieurs.

14. Le Mandataire fournit, sur simple demande du Mandant, une attestation écrite de suppression.

Toute conservation au-delà de la période susmentionnée nécessite une instruction écrite du Mandant ou résulte d'une obligation légale impérative.

12. Audit et contrôle

Le Mandant peut, à ses frais et sous préavis raisonnable de trente (30) jours, procéder à un audit ou faire procéder à un audit par un tiers indépendant soumis à une obligation de confidentialité, afin de vérifier le respect du présent DPA.

Le Mandataire fournit, sur demande, toute documentation pertinente justifiant sa conformité (registre des traitements, certifications de ses sous-traitants, rapports d'incidents).

Si l'audit révèle un manquement substantiel imputable au Mandataire, les frais d'audit sont mis à la charge de ce dernier.

13. Responsabilité

Chaque partie est responsable des manquements qui lui sont imputables. Le Mandataire répond des violations résultant d'une faute, d'une négligence ou d'un manquement à ses obligations contractuelles ou légales.

La responsabilité financière du Mandataire est limitée, par sinistre et par année civile, au montant total des honoraires versés par le Mandant au cours des six (6) mois précédant le fait générateur, sauf en cas de faute intentionnelle ou de négligence grave.

14. Loi applicable et juridiction

Le présent DPA est soumis au droit suisse, à l'exclusion des règles de conflit de lois.

Tout litige relatif à l'interprétation ou à l'exécution du présent DPA relève de la compétence exclusive des tribunaux du canton de Vaud, Suisse, sous réserve d'un recours au Tribunal fédéral.

Lorsque le RGPD s'applique au traitement, les personnes concernées peuvent également faire valoir leurs droits devant les juridictions de leur lieu de résidence habituelle au sein de l'Union européenne.

Acceptation du présent DPA

Le présent DPA est accepté par voie électronique par le Mandant lors de la souscription, en même temps que les Conditions générales dont il constitue une annexe intégrante. Cette acceptation est enregistrée et horodatée par le prestataire de paiement. Conformément à l'article 28 par. 9 du RGPD, qui admet expressément la forme électronique, et au droit suisse qui n'impose aucune forme particulière pour un tel accord, cette acceptation vaut conclusion par écrit. Le présent DPA prend effet à la date de la souscription et reste applicable pendant toute la durée du Contrat de Mandat.

Copie signée — Le Mandant qui souhaite disposer d'un exemplaire signé par les deux parties peut en faire la demande à carine@cara-global.ch. Un exemplaire lui est alors adressé pour signature, sans que cela conditionne l'entrée en vigueur du présent DPA.