
Accord de traitement de données

● Version 1.0 • Entrée en vigueur : 15 septembre 2026

Le présent accord est conclu en application de l'article 28 du règlement (UE) 2016/679, ci-après « le RGPD ».

Entre

L'organisation utilisatrice du service REPERES, ci-après « le Responsable de traitement »,

Et

La société **BARBAUX MORALES SOLUTIONS ET EXPERTISE (BMSE)**, SARL au capital de 1 000 euros, 3B rue des Jardiniers, 67190 Mutzig, SIREN 990 220 907, RCS Saverne, ci-après « le Sous-traitant ».

Le présent accord s'applique dès lors que le Responsable de traitement utilise REPERES pour traiter des données personnelles dont il détermine les finalités et les moyens. Il fait partie intégrante des conditions générales d'utilisation et prévaut sur celles-ci pour ce qu'il régit.

Article 1 — Objet et périmètre

Le Sous-traitant traite des données personnelles pour le compte du Responsable de traitement, dans la seule mesure nécessaire à la fourniture du service REPERES.

Le service est conçu pour être utilisé sans transmission d'éléments identifiants relatifs aux personnes accompagnées. Les conditions générales d'utilisation interdisent de façon absolue au Responsable de traitement et à ses utilisateurs de transmettre les identifiants directs d'une personne accompagnée, de sa famille ou d'un tiers, ainsi que toute pièce de dossier individuel non expurgée. Elles imposent en outre une obligation de minimisation et de vigilance sur la combinaison des éléments transmis, et mettent à disposition une fonction de protection avec prévisualisation avant envoi. La description d'une situation professionnelle en termes généraux constitue en revanche l'usage même du service.

Le présent accord régit en conséquence :

1. les données personnelles des **utilisateurs** rattachés au Responsable de traitement, traitées pour la gestion des accès et le fonctionnement du service ;
2. les données personnelles qui, en dépit de l'interdiction rappelée ci-dessus, seraient contenues dans une requête ou dans une pièce jointe transmise au service.

Article 2 — Description du traitement

Nature des opérations : réception, transmission, transformation en mémoire, recherche documentaire, génération de texte, effacement.

Finalité : fourniture du service d'assistance documentaire et rédactionnelle.

Durée : la durée de l'accès du Responsable de traitement au service.

Catégories de personnes concernées : les utilisateurs rattachés au Responsable de traitement ; incidemment, toute personne mentionnée dans une requête en méconnaissance des conditions générales d'utilisation.

Catégories de données :

CATÉGORIE	CONTENU	CONSERVATION
Identification des utilisateurs	Adresse électronique, nom d'affichage, identifiant d'authentification	Durée de l'accès, puis 30 jours
Gestion des accès	Rattachement, rôle, droits, dates	Durée de l'accès
Justificatifs d'éligibilité	Documents transmis par le Responsable de traitement	Durée du droit, plus un an
Demandes adressées au support	Objet, message, adresse de réponse, pièces jointes	3 ans à compter de la clôture
Métadonnées d'usage	Horodatage, origine, indicateur d'authentification, thème de qualification	13 mois
Contenu des requêtes	Traité en mémoire uniquement	Non conservé

Article 3 — Non-conservation du contenu des requêtes

Le Sous-traitant garantit qu'aucune requête, aucune réponse générée, aucun document joint et aucun historique de conversation n'est enregistré, ni dans ses bases de données, ni dans ses journaux techniques, ni dans ses systèmes de sauvegarde.

Le traitement d'une requête s'effectue intégralement en mémoire vive. Les seules traces persistantes sont les métadonnées d'usage décrites à l'article 2, qui ne comportent aucun élément du contenu.

Cette garantie s'étend aux chemins d'erreur : aucun contenu de requête n'est journalisé, y compris en cas d'échec technique.

Article 4 — Instructions documentées

Le Sous-traitant ne traite les données que sur instruction documentée du Responsable de traitement. Les conditions générales d'utilisation, les annexes applicables et le présent accord constituent ces instructions.

Le Sous-traitant informe le Responsable de traitement s'il estime qu'une instruction constitue une violation du RGPD ou d'une autre disposition applicable en matière de protection des données.

Le Sous-traitant ne traite les données à ses propres fins que dans les limites suivantes, pour lesquelles il agit en qualité de responsable de traitement autonome : gestion de la relation contractuelle, facturation, sécurité du service, et exploitation de métadonnées d'usage agrégées et dépourvues de contenu aux fins de pilotage de la capacité et de la qualité.

Article 5 — Confidentialité

Le Sous-traitant veille à ce que les personnes autorisées à traiter les données s'engagent au respect de la confidentialité et reçoivent la formation nécessaire.

L'accès aux données des Responsables de traitement est limité à une liste nominative d'opérateurs, dont chaque action sensible est soumise à motif obligatoire et inscrite à un journal d'audit non modifiable.

Article 6 — Sécurité

Les mesures techniques et organisationnelles mises en œuvre figurent en **annexe 1**. Le Sous-traitant peut les faire évoluer, sous réserve de ne pas en diminuer le niveau global.

Article 7 — Sous-traitance ultérieure

Le Responsable de traitement autorise de manière générale le recours aux sous-traitants ultérieurs listés en **annexe 2**.

Le Sous-traitant informe le Responsable de traitement de tout ajout ou remplacement de sous-traitant ultérieur **au moins soixante jours avant** que le changement ne prenne effet, par message électronique adressé à l'administrateur de l'organisation et par publication sur le service.

Le Responsable de traitement peut s'opposer au changement, par écrit et de façon motivée, dans un délai de trente jours. En cas d'opposition maintenue, il peut résilier son accès sans frais, avec remboursement au prorata pour un accès payant.

Le Sous-traitant impose à chaque sous-traitant ultérieur les mêmes obligations que celles du présent accord et demeure pleinement responsable de leur exécution.

Article 8 — Localisation et transferts

L'intégralité des traitements est réalisée sur le territoire de la République française.

Aucun transfert de données hors de l'Union européenne n'est effectué, ni par le Sous-traitant, ni par ses sous-traitants ultérieurs, dans le cadre du service.

Tout projet de transfert hors de l'Union européenne serait soumis à la procédure d'information et d'opposition prévue à l'article 7.

Article 9 — Assistance au Responsable de traitement

Droits des personnes concernées. Le Sous-traitant met à disposition du Responsable de traitement les fonctions permettant de répondre aux demandes d'exercice de droits portant sur les comptes des utilisateurs rattachés. Si une demande lui est adressée directement, il la transmet sans délai au Responsable de traitement sans y répondre lui-même.

Le Responsable de traitement est informé que **le contenu des requêtes n'étant pas conservé, il ne peut faire l'objet ni d'une communication, ni d'une rectification, ni d'un effacement.**

Autres obligations. Le Sous-traitant assiste le Responsable de traitement, compte tenu de la nature du traitement et des informations dont il dispose, pour la sécurité, la notification de violations, les analyses d'impact et la consultation préalable de l'autorité de contrôle.

Article 10 — Violation de données

Le Sous-traitant notifie au Responsable de traitement toute violation de données personnelles le concernant **dans les meilleurs délais et au plus tard quarante-huit heures** après en avoir pris connaissance.

La notification décrit la nature de la violation, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, les conséquences probables, les mesures prises ou proposées, et un point de contact.

Lorsque toutes les informations ne peuvent être fournies simultanément, elles le sont de manière échelonnée, sans délai indu.

Le Sous-traitant ne notifie pas l'autorité de contrôle ni les personnes concernées à la place du Responsable de traitement.

Article 11 — Sort des données en fin de contrat

À la fin de la fourniture du service, le Sous-traitant supprime les données personnelles du Responsable de traitement dans un délai de **trente jours**, sauf obligation légale de conservation.

Le Responsable de traitement peut demander, avant l'expiration de ce délai, la restitution des données de gestion des accès dans un format structuré et couramment utilisé.

Les données figurant dans les sauvegardes sont supprimées à l'expiration du cycle de rotation, dans un délai maximal de quatre-vingt-dix jours. Pendant cet intervalle, elles ne font l'objet d'aucun traitement actif.

Article 12 — Audit

Le Sous-traitant met à disposition du Responsable de traitement les informations nécessaires pour démontrer le respect des obligations du présent accord, notamment la présente annexe 1, la liste actualisée des sous-traitants ultérieurs et, sur demande, les attestations et certifications de ses hébergeurs.

Le Responsable de traitement peut réaliser un audit, par lui-même ou par un auditeur mandaté n'étant pas un concurrent du Sous-traitant, dans la limite d'**un audit par période de douze mois**, sauf incident de sécurité avéré.

L'audit fait l'objet d'un préavis de trente jours, se déroule pendant les heures ouvrées, ne perturbe pas le service et respecte la confidentialité des données des autres clients. Ses frais sont à la charge du Responsable de traitement, sauf si l'audit révèle un manquement substantiel.

Article 13 — Responsabilité et durée

Chaque partie répond des dommages causés par un traitement effectué en violation du RGPD, dans les conditions de son article 82.

Le présent accord entre en vigueur à l'ouverture de l'accès et demeure applicable pendant toute sa durée, ainsi que, pour les articles 5, 8 et 11, jusqu'à la suppression effective des données.

Annexe 1 — Mesures techniques et organisationnelles

Architecture

- Hébergement intégral en France, région fr-par, chez Scaleway.
- Une passerelle applicative constitue l'unique point d'entrée de confiance. Le moteur de traitement, la base de données et le service de protection des données ne sont pas exposés publiquement.
- Cloisonnement applicatif par organisation, appliqué par la passerelle.

Chiffrement

- Chiffrement des communications en transit, HTTPS imposé.
- Chiffrement des données au repos, en base de données et en stockage d'objets.

Contrôle d'accès

- Authentification par fournisseur d'identité dédié, en OpenID Connect, avec cookies de session strictement techniques.
- Accès au service de gestion pour un rôle applicatif limité aux opérations de manipulation de données, sans droit de modification de structure.
- Espace d'administration réservé à une liste nominative d'opérateurs. Motif obligatoire et journalisation avant et après pour toute action sensible.
- Clés d'accès programmatiques stockées sous forme d'empreinte, révocables à effet immédiat.

Stockage des pièces jointes

- Espace de stockage privé, aucun objet accessible sans signature.
- Accès par liens temporaires d'une durée de dix minutes.
- Noms de fichiers assainis, clés de stockage sans lien avec le nom d'origine.

Journalisation et traçabilité

- Aucun contenu de requête, de réponse ou de document dans les journaux techniques, y compris sur les chemins d'erreur.
- Journal d'audit des actions sensibles, conservé trois ans.

Minimisation

- Traitement des requêtes en mémoire vive, sans persistance.
- Fonction de protection des données personnelles disponible dans l'interface web, à l'initiative de l'utilisateur.
- Métadonnées d'usage dépourvues de tout contenu.

Effacement

- Tâche automatique d'application des durées de conservation, exécutée périodiquement, supprimant objets et enregistrements arrivés à échéance, et inscrite au journal d'audit.

Disponibilité et intégrité

- Sauvegarde automatique quotidienne des bases par l'hébergeur, avec une rétention de sept jours et restauration possible depuis la console d'administration. Un export complémentaire au format pg_dump peut être réalisé à la demande.
- Limitation du nombre de requêtes par minute et par adresse.
- Supervision de l'état du service et de ses composants.

Gestion des secrets

- Secrets applicatifs gérés par un service dédié, jamais versionnés.

Annexe 2 — Sous-traitants ultérieurs

SOUS-TRAITANT	RÔLE	LOCALISATION DU TRAITEMENT
Scaleway SAS, France	Hébergement applicatif, base de données, stockage d'objets, service d'indexation documentaire, envoi de messages transactionnels, gestion des secrets	France, fr - par
Mistral AI SAS, France	Modèles de langage : qualification, classement des extraits, génération de réponses, lecture optique de documents	France
ConfidensIA SAS, France	Fonction de protection des données personnelles	France, sur infrastructure Scaleway
Stripe Payments Europe, Limited, Irlande	Traitement des paiements pour les accès payants	Union européenne

Le modèle employé pour la génération des réponses les plus complexes est un modèle à poids ouverts d'origine tierce, servi par Mistral AI sur son infrastructure située en France. Son auteur n'intervient pas dans la chaîne de traitement et ne reçoit aucune donnée.

Cette annexe est tenue à jour. Toute modification est soumise à la procédure de l'article 7.

Annexe 3 — Contacts

Contact du Sous-traitant en matière de protection des données	dpo@bmse.fr
Contact du Responsable de traitement	Renseigné par l'organisation dans son espace
Adresse de notification des violations	Adresse de l'administrateur de l'organisation