

Accord de sous-traitance (DPA)

Version 2.1 — 29 août 2026

CE QUI A CHANGÉ

Liste des sous-traitants ultérieurs mise à jour et restructurée en trois familles. Ajout de Mistral AI (vectorisation pour la recherche sémantique), Unipile (messagerie hébergée) et Browserbase (navigateur hébergé), auparavant couverts par la seule mention générique. Stancer remplacé par Mollie, et Pennylane ajouté (facturation) — tous deux désormais présentés comme prestataires de l'Éditeur pour sa propre facturation. Ajout de l'authentification à deux facteurs exigible par organisation et du liage cryptographique des secrets à leur ligne dans les mesures de sécurité. Centre de confiance déplacé sur trust.oto.zone.



Objet & rôles

En bref : Cet accord encadre, au titre de l'article 28 du RGPD, le traitement des données personnelles réalisé par oto pour le compte de ses clients. Le Client est responsable de traitement ; l'Éditeur est sous-traitant.

Le présent accord de sous-traitance (« DPA », version 2.1) complète les **conditions d'abonnement** et encadre, conformément à l'**article 28 du RGPD**, les traitements de données à caractère personnel effectués par l'Éditeur (Otomata, SASU immatriculée au RCS de Marseille, SIREN 106 974 637, TVA intracommunautaire FR05106974637 — le « sous-traitant ») pour le compte du Client (le « responsable de traitement »).

Objet et durée : fourniture de la plateforme d'automatisation oto, pour la durée de l'abonnement. **Nature et finalité :** hébergement, exécution des automatisations demandées par le Client et ses agents, indexation des contenus du Client pour les rendre recherchables, conservation chiffrée des secrets de connexion. **Catégories de personnes concernées et de données :** déterminées par le Client selon les outils qu'il connecte et les traitements qu'il déclenche. Le sous-traitant traite ces données **sur instruction documentée** du responsable et ne les utilise à aucune autre fin.

Ce que cet accord ne couvre pas. L'Éditeur agit en **responsable de traitement pour son propre compte** sur les traitements qui lui sont propres : gestion du compte et de l'organisation, identité et contact de facturation, encaissement et facturation de l'abonnement, trace horodatée de l'acceptation des documents contractuels. Ces traitements sont décrits dans la **politique de confidentialité** et dans les **conditions générales de vente**.

Une version signable de cet accord est mise à disposition des clients sur trust.oto.zone.



Sous-traitants ultérieurs

En bref : Le responsable autorise le recours aux sous-traitants ultérieurs listés ci-dessous et est informé de tout changement, avec possibilité de s'y opposer.

Le responsable de traitement autorise l'Éditeur à recourir aux sous-traitants ultérieurs suivants, chacun encadré par un contrat conforme à l'article 28 :

Scaleway — Hébergement, base de données, stockage objet, gestion de secrets, e-mail transactionnel — Union européenne (France)

Logto — Authentification (auto-hébergé par l'Éditeur chez Scaleway) — Union européenne (France)

Mistral AI — Vectorisation du texte des pages, documents et fichiers du Client, aux seules fins de la recherche sémantique au sein de la plateforme (modèle `mistral-embed`, mode API, sans entraînement sur les contenus soumis) — Union européenne (France)

Sentry — Supervision et journalisation des erreurs techniques (peut contenir des données personnelles) — Union européenne (Allemagne)

PostHog — Mesure d'audience du site et du tableau de bord, uniquement après consentement — Union européenne

Anthropic (Claude) — Assistant IA utilisé par les équipes de l'Éditeur pour l'exploitation, le support et l'accompagnement (susceptible, à cette occasion, de traiter ponctuellement des données client) — mode API sans entraînement sur les contenus soumis ; transferts hors UE encadrés par clauses contractuelles types — États-Unis

L'Éditeur informe le responsable de tout ajout ou remplacement de sous-traitant ultérieur, en lui laissant un délai raisonnable pour s'y opposer pour des motifs légitimes.



Services de connecteurs

En bref : Certains connecteurs reposent sur des services tiers, mobilisés uniquement si vous les activez et les utilisez. Les deux principaux sont nommés ci-dessous ; la liste à jour vit sur trust.oto.zone.

oto se connecte à des outils tiers. Deux cas se distinguent, et ils n'ont pas le même régime :

Vos propres accès. Lorsque vous connectez un outil avec **votre propre clé ou votre propre compte** (le cas le plus fréquent du catalogue), oto exécute votre instruction en appelant un service avec lequel **vous êtes déjà en relation contractuelle**. L'Éditeur n'y ajoute pas de sous-traitant : il transporte votre requête et votre identifiant, qu'il conserve chiffré.

Les services que l'Éditeur met à disposition. Certains connecteurs reposent sur un service tiers contracté par l'Éditeur, mobilisé **uniquement si vous activez et utilisez ce connecteur** :

Unipile — Messagerie hébergée : la session de votre compte de messagerie ou de réseau social (LinkedIn, WhatsApp, Telegram, Instagram, Messenger, X) est opérée chez Unipile, qui traite à cette occasion vos messages et les données de vos correspondants — Union européenne (France)

Browserbase — Navigateur hébergé, pour lire un site derrière authentification depuis une session que vous ouvrez vous-même ; il détient le profil de session correspondant — États-Unis ; transferts encadrés par clauses contractuelles types

Autres services de connecteurs — d'autres connecteurs (données d'entreprise, enrichissement, recherche) peuvent s'appuyer sur des services tiers contractés par l'Éditeur et pouvant opérer hors de l'Union européenne, encadrés par clauses contractuelles types

La **liste à jour** de ces services, avec leur rôle et leur localisation, est publiée sur trust.oto.zone. L'Éditeur y applique le même engagement d'information préalable et de droit d'opposition qu'aux sous-traitants ultérieurs.



Prestataires de facturation de l'Éditeur

En bref : L'encaissement et la facturation de l'abonnement relèvent des traitements propres à l'Éditeur. Ils sont mentionnés ici pour information : Mollie encaisse, Pennylane émet les factures.

Les traitements ci-dessous sont ceux de l'**Éditeur agissant pour son propre compte** — ils ne portent pas sur les données que le Client confie à la plateforme. Ils sont mentionnés ici pour la complète information du responsable de traitement :

Mollie B.V. — Encaissement des abonnements ; établissement de monnaie électronique agréé et supervisé par la banque centrale des Pays-Bas (De Nederlandsche Bank) — Pays-Bas (Union européenne)

Pennylane — Émission des factures et avoirs d'abonnement, sur la comptabilité de l'Éditeur ; traite l'identité et le contact de facturation du Client — Union européenne (France)



Mesures de sécurité

En bref : Chiffrement au repos des secrets (AES-256-GCM), clé maîtresse hors base, isolation par utilisateur, authentification à deux facteurs exigible par organisation, révocation à plusieurs niveaux. [Détail sur trust.oto.zone](https://trust.oto.zone).

L'Éditeur met en œuvre des mesures techniques et organisationnelles appropriées (article 32 du RGPD) :

Chiffrement au repos des secrets et identifiants de connexion (AES-256-GCM), avec **clé maîtresse conservée hors base** et jamais écrite en clair sur disque. Chaque secret chiffré est **lié cryptographiquement à sa ligne** : un secret ne peut pas être transplanté vers un autre connecteur ni vers une autre organisation.

Isolation par utilisateur des secrets et cloisonnement par organisation.

Authentification par OAuth 2.0 / PKCE (Logto self-hosted), transport chiffré de bout en bout (TLS). Une organisation peut **exiger l'authentification à deux facteurs** de ses membres.

Révocation à plusieurs niveaux : retrait d'un accès utilisateur, suppression d'un credential d'organisation.

Connecteurs distants (« bridges ») à privilèges restreints pour les accès sensibles (lecture seule selon le déploiement) : le credential client vit dans un service isolé, jamais dans la plateforme. *Option* : ce service est hébergeable dans l'infrastructure du client (le credential ne quitte alors pas son cloud) — proposé au cas par cas, ce n'est pas la configuration par défaut.

Le détail des mesures, leur état de déploiement et le durcissement en cours sont publiés sur trust.oto.zone. L'Éditeur notifie le responsable de toute violation de données concernant ses données dans les meilleurs délais après en avoir pris connaissance.



Hébergement & localisation

En bref : Données hébergées dans l'Union européenne (France, Scaleway). Les transferts éventuels hors UE sont encadrés par des clauses contractuelles types.

Les données du Client sont hébergées dans l'**Union européenne** (France, région Scaleway fr-par) : base de données managée, stockage objet, coffre de secrets, e-mail transactionnel.

Deux sous-traitants opèrent **hors de l'Union européenne** : **Anthropic** (outillage d'exploitation de l'Éditeur) et **Browserbase** (navigateur hébergé, connecteur optionnel), tous deux aux États-Unis. D'autres services de connecteurs optionnels peuvent également opérer hors de l'Union. Dans tous ces cas, les transferts sont encadrés par les garanties appropriées prévues par le RGPD (**clauses contractuelles types** de la Commission européenne, mesures complémentaires le cas échéant).



Droits & obligations du responsable

En bref : Assistance aux demandes des personnes, notification des violations, audit, et suppression ou restitution des données en fin de contrat.

L'Éditeur, en tant que sous-traitant, s'engage à :

Instructions — Ne traiter les données que sur instruction documentée du responsable.

Confidentialité — Garantir la confidentialité des données et l'engagement de confidentialité des personnes autorisées à les traiter.

Assistance — Aider le responsable à répondre aux demandes d'exercice de droits des personnes concernées, et à respecter ses obligations de sécurité et de notification.

Violations — Notifier le responsable de toute violation de données dans les meilleurs délais.

Audit — Mettre à disposition les informations nécessaires pour démontrer le respect de l'article 28 et permettre des audits raisonnables.

Fin de contrat — Supprimer ou restituer les données au choix du responsable en fin de prestation, sauf obligation légale de conservation. La résiliation d'un abonnement ou sa fermeture pour impayé n'entraîne, à elle seule, **aucune suppression de données** : elle ferme les droits d'accès aux fonctionnalités payantes.

Le responsable de traitement, de son côté, garantit disposer d'une base légale pour les traitements qu'il déclenche via oto et pour les données qu'il connecte.

Le présent DPA fait partie intégrante des [conditions d'abonnement](#) et est régi par le droit français. Une version signable est disponible sur trust.oto.zone.