

ANNEXE DONNÉES ET SÉCURITÉ

Version 1.8, à jour du 14 juin 2026

PRÉAMBULE ET OBJET

La présente annexe complète et fait partie intégrante des Conditions Générales de Service Azuro AI. Elle vaut **accord de sous-traitance au sens de l'article 28 du Règlement (UE) 2016/679 (RGPD)** et précise les modalités de traitement des données, d'hébergement, de sécurité et de confidentialité applicables au Service. Elle est mise à disposition du Client en annexe des Conditions Générales et lui est transmise sur demande.

Les termes commençant par une majuscule ont le sens qui leur est donné dans les Conditions Générales.

PARTIE 1. ACCORD DE SOUS-TRAITANCE (ARTICLE 28 RGPD)

1.1 Rôles des parties

Le Client est **responsable de traitement** : il détermine les finalités et les moyens des traitements qu'il met en oeuvre au moyen de l'AIOS, ainsi que les données qu'il y dépose et y crée. Azuro est **sous-traitant** : il traite les données pour le compte du Client, dans la limite de la fourniture du Service, sans en déterminer les finalités.

1.2 Description du traitement

- **Nature et finalité** : fourniture du Service (mise à disposition de l'AIOS, hébergement du VPS, mises à jour, support).
- **Catégories de données** : les données déposées et créées par le Client dans l'AIOS, dont la nature est librement déterminée par le Client et peut inclure des données à caractère personnel.
- **Catégories de personnes concernées** : déterminées par le Client en fonction de l'usage qu'il fait du Service.
- **Durée** : la durée de la relation contractuelle.

1.3 Obligations d'Azuro

Azuro s'engage à :

- a) ne traiter les données que sur **instruction documentée** du Client, sauf obligation légale ;
- b) veiller à ce que les personnes autorisées à traiter les données s'engagent à la **confidentialité** ;
- c) mettre en oeuvre les **mesures techniques et organisationnelles appropriées** (article 32 RGPD), décrites en Partie 4 ;
- d) ne recourir à un **sous-traitant ultérieur** que dans les conditions de la Partie 2 (information du Client et possibilité d'opposition) ;
- e) **assister** le Client, dans la mesure du possible, pour répondre aux demandes d'exercice des droits des personnes concernées ;
- f) **assister** le Client pour le respect de ses obligations en matière de sécurité, de notification des violations et d'analyses d'impact ;
- g) au choix du Client, **restituer ou supprimer** les données au terme de la relation, dans les conditions de la Partie 5 ;

h) mettre à la disposition du Client les **informations nécessaires** pour démontrer le respect des obligations du présent article ;

i) **notifier** au Client toute violation de données dans les conditions de la Partie 6.

1.4 Obligations du Client

Le Client s'engage à disposer d'une base légale pour les traitements qu'il met en oeuvre, à ne donner que des instructions licites, à informer les personnes concernées lorsque cela est requis, et à ne déposer dans l'AIOS que des données qu'il est en droit de traiter.

PARTIE 2. SOUS-TRAITANTS ET TIERS

2.1 Sous-traitants ultérieurs d'Azuro

Pour la fourniture du Service, Azuro recourt aux sous-traitants suivants :

- **Hébergement** : Hostinger, qui fournit l'infrastructure du VPS. Hébergement situé en France par défaut (Partie 4).
- **Paiement** : Stripe, qui assure le traitement des paiements et la facturation (données de facturation : identité, adresse, adresse électronique, numéro de TVA le cas échéant).
- **Sauvegarde hors-site** : GitHub, qui héberge les deux dépôts privés de sauvegarde dédiés au Client (Workspace et système), dans les conditions de la Partie 4.

Azuro se réserve le droit de faire évoluer ces sous-traitants dans les conditions de l'article 2.3.

2.2 Modèle d'intelligence artificielle

Le modèle d'intelligence artificielle utilisé par l'AIOS est, à ce jour, celui d'Anthropic (Claude). Il est mobilisé **au moyen de l'abonnement personnel du Client** auprès de ce fournisseur. La relation relative à ce service, ainsi que les conditions qui lui sont applicables, relèvent du **Client et du fournisseur**.

Azuro **n'utilise pas le contenu du Client pour entraîner un quelconque modèle d'intelligence artificielle**. Les conditions applicables à l'utilisation des données par le fournisseur du modèle, y compris en matière d'entraînement, relèvent des conditions de ce fournisseur applicables à l'abonnement du Client.

Azuro se réserve le droit de prendre en charge d'autres fournisseurs de modèle d'IA.

2.3 Information et opposition

Azuro informe le Client de tout projet de changement concernant ses sous-traitants ultérieurs. Le Client peut s'y opposer pour un motif légitime.

PARTIE 3. CONFIDENTIALITÉ ET ACCÈS

3.1 Engagement de confidentialité

Azuro et les personnes qui interviennent pour son compte sont tenus à une obligation de **confidentialité** sur les données du Client. Cette obligation survit à la fin de la relation contractuelle.

3.2 Accès opérateur

L'accès d'Azuro au VPS du Client est **limité au strict nécessaire** aux opérations de maintenance et de correction d'anomalies. Les données d'un Client ne sont pas accessibles depuis l'instance d'un autre Client (**cloisonnement**). Conformément aux Conditions Générales, cet accès peut être interrompu à la demande du Client.

PARTIE 4. HÉBERGEMENT ET SÉCURITÉ

4.1 Hébergement et localisation

L'AIOS est déployé sur un **VPS dédié au Client** (architecture isolée, un serveur par Client). L'hébergement est situé **en France** par défaut. Un autre emplacement peut être retenu à la demande du Client, dans la limite des emplacements disponibles.

4.2 Sécurité en transit

Les communications entre le Client, l'AIOS et les services tiers sont **chiffrées en transit** (HTTPS / TLS). Les connexions en clair sont redirigées vers le canal chiffré.

4.3 Sécurité des données au repos

La protection des données stockées sur le VPS du Client repose sur une **défense en couches** :

- **Isolation mono-tenant** : un VPS est dédié à chaque Client. Aucune donnée n'est partagée entre Clients et les données d'un Client ne sont pas accessibles depuis l'instance d'un autre.
- **Restriction d'accès aux secrets** : les fichiers contenant des secrets (identifiants, jetons, clés techniques) sont stockés avec des **permissions restreintes au seul compte administrateur** du serveur.
- **Contrôle d'accès durci** : l'accès à l'application est protégé dans les conditions de l'article 4.4.
- **Chiffrement en transit** : les échanges sont chiffrés conformément à l'article 4.2.
- **Sauvegardes hors-site chiffrées** : les copies hors-site sont conservées sur une infrastructure qui en assure le chiffrement au repos, dans les conditions de l'article 4.5.

4.4 Authentification et contrôle d'accès

L'accès à l'application est protégé par les mesures suivantes :

- **Mot de passe non conservé en clair** : le mot de passe d'accès est vérifié au moyen d'un **condensat cryptographique** (haché), et n'est pas conservé en clair.
- **Limitation des tentatives de connexion** : un mécanisme bloque temporairement les tentatives de connexion répétées, en **protection contre les attaques par force brute**.
- **Cookie de session sécurisé** : le cookie de session est transmis **uniquement sur un canal chiffré** (attribut Secure), n'est pas accessible au code de la page (HttpOnly) et est restreint au site (SameSite).
- **Authentification à deux facteurs en option** : le Client peut activer une **double authentification** par code temporaire (TOTP), assortie de codes de secours à usage unique.

4.5 Sauvegardes

Le Service comprend un dispositif de **sauvegarde à plusieurs niveaux**, destiné à permettre la **récupération des données en cas de perte** :

- **Sur le VPS** : une sauvegarde du Workspace et de l'AIOS est réalisée chaque jour sur le VPS lui-même, ce qui permet une restauration rapide en cas de fausse manipulation ou de perte de données.
- **Hors-site** : une copie est répliquée chaque jour sur GitHub, dans deux dépôts privés dédiés au Client (l'un pour le Workspace, l'autre pour le système), sous le contrôle d'Azuro, afin de permettre une restauration même en cas de défaillance du VPS.
- **Au niveau du prestataire d'hébergement** : le prestataire d'hébergement réalise en outre, de façon périodique, sa propre sauvegarde du serveur.

Ces sauvegardes sont activées par défaut et peuvent être **désactivées à la simple demande** du Client.

PARTIE 5. CONSERVATION, RESTITUTION ET SUPPRESSION

5.1 Durées de conservation

Les durées de conservation appliquées sont les suivantes :

- **Données de service** (contenu du Workspace, conversations, pièces jointes, paramètres, mémoire) : conservées pendant **toute la durée de la relation contractuelle**. Elles ne font pas l'objet d'une purge liée à leur ancienneté ; elles sont supprimées au terme de la relation (article 5.3) ou à la demande du Client (article 5.4 et article 8 des Conditions Générales).
- **Journaux applicatifs** : conservés pour une durée **maximale de 180 jours (six mois)**, avec rotation puis **purge automatique** au-delà de cette durée.
- **Marqueurs techniques de session** : 90 jours.
- **Journaux de session internes** : 180 jours.

Ces durées sont appliquées **automatiquement**.

5.2 Restitution et export autonome

À tout moment en cours de relation, le Client peut **exporter lui-même** depuis l'application, et sans intervention d'Azuro, l'intégralité de ses données (Workspace, conversations, paramètres, mémoire, pièces jointes et historique d'acceptation des documents contractuels), sous la forme d'une archive en **formats ouverts**. Cette fonction demeure disponible y compris en cas d'abonnement expiré, afin de garantir la réversibilité.

Au terme de la relation, Azuro restitue en outre au Client l'intégralité du contenu de son VPS (Workspace et AIOS tel que configuré par le Client), en formats ouverts.

5.3 Suppression

Au terme de la relation, ou à la demande du Client en cours de relation, Azuro procède à la **suppression définitive** des données, **après confirmation du Client**. Lorsque la demande intervient en cours de relation, la suppression est réalisée dans un **délai maximum de trente (30) jours**. Une **attestation de suppression** est remise au Client.

5.4 Demande de suppression par le Client

Le Client peut, depuis l'application, demander la suppression de l'ensemble de ses données. La demande fait l'objet d'une **confirmation préalable** (avec possibilité d'exporter d'abord ses données), reste **annulable** tant qu'elle n'a pas été exécutée, et donne lieu à la remise d'une attestation de suppression dans les conditions de l'article 5.3.

PARTIE 6. NOTIFICATION DES VIOLATIONS DE DONNÉES

En cas de violation de données susceptible d'affecter les données du Client, Azuro en informe le Client **dans les meilleurs délais** et l'assiste, dans la mesure du possible, dans la gestion de l'incident.

PARTIE 7. DURÉE ET ARTICULATION

La présente annexe s'applique pendant toute la durée des Conditions Générales, auxquelles elle est subordonnée et dont elle suit le sort. Les engagements de confidentialité survivent à son terme.