

ACCORD DE TRAITEMENT DES DONNÉES PERSONNELLES (DPA)

Annexe Contractuelle Obligatoire relative à la protection des données (Règlement UE 2016/679 - RGPD)

Le présent Accord de Traitement des Données (ci-après le « **DPA** ») fait partie intégrante des Conditions Générales de Vente et de Prestations de Services (CGV) ou du contrat conclu entre **AITRPRO** (ci-après le « Sous-traitant ») et son **Client** (ci-après le « Responsable du traitement »). Il a pour objet de définir les conditions dans lesquelles AITRPRO s'engage à effectuer, pour le compte du Client, les opérations de traitement de données à caractère personnel définies à l'Annexe 1.

Exclusion : Le présent DPA ne s'applique pas aux traitements pour lesquels AITRPRO détermine ses propres finalités (notamment la gestion de la relation commerciale B2B, la facturation, la comptabilité et ses obligations légales), pour lesquels AITRPRO agit en qualité de Responsable du traitement indépendant.

ARTICLE 1 – QUALIFICATION ET OBLIGATIONS DU CLIENT

Dans le cadre de l'exécution des prestations d'infogérance, télémaintenance, administration cloud ou sauvegarde, AITRPRO agit exclusivement pour le compte du Client. À ce titre, le Client revêt la qualité de **Responsable du traitement** et AITRPRO celle de **Sous-traitant** (art. 28 RGPD).

Le Client demeure seul responsable de la détermination des finalités et des moyens essentiels des traitements, de leur licéité, de l'information des personnes concernées et, le cas échéant, de la collecte de leur consentement. Il s'engage à ne transmettre à AITRPRO que des instructions licites et documentées, et à lui fournir toutes les informations nécessaires à la bonne exécution des prestations.

ARTICLE 2 – INSTRUCTIONS DOCUMENTÉES D'AITRPRO

AITRPRO s'engage à ne traiter les données personnelles que sur **instruction documentée** du Client. Le contrat d'infogérance, le devis validé, et les demandes de support via le système de ticketing (Helpdesk) ou par email constituent les instructions documentées du Client.

Si AITRPRO considère qu'une instruction constitue une violation du RGPD ou d'une autre disposition applicable en matière de protection des données, elle en informe immédiatement le Client et peut suspendre l'exécution de l'instruction concernée dans l'attente de sa mise en conformité.

ARTICLE 3 – CONFIDENTIALITÉ ET SÉCURITÉ

3.1 Confidentialité : AITRPRO s'assure que son personnel (techniciens, ingénieurs) autorisé à traiter les données personnelles est soumis à une stricte obligation de confidentialité contractuelle ou légale, et reçoit la formation nécessaire en matière de protection des données.

3.2 Mesures de sécurité : AITRPRO met en œuvre les mesures techniques et organisationnelles (TOMs) appropriées afin de garantir un niveau de sécurité adapté au risque. Ces mesures, détaillées en **Annexe 2**, visent à protéger les données contre la destruction, la perte, l'altération ou la divulgation non autorisée, notamment via le chiffrement, la gestion stricte des habilitations et la journalisation (AISentinel).

ARTICLE 4 – ASSISTANCE (ART. 32 À 36 RGPD) ET DROITS DES PERSONNES

Compte tenu de la nature du traitement et des informations dont elle dispose, AITRPRO assiste raisonnablement le Client pour lui permettre de satisfaire aux obligations résultant des articles 32 à 36 du RGPD, notamment en matière de sécurité, gestion des violations de données, analyses d'impact (AIPD) et consultation préalable de l'autorité de contrôle.

Il appartient au Client de gérer les demandes d'exercice de droits des personnes concernées (accès, rectification, effacement). AITRPRO assistera le Client, par des mesures techniques appropriées, pour donner suite à ces demandes. Toute demande reçue directement par AITRPRO sera transmise sans délai au Client.

ARTICLE 5 – NOTIFICATION DES VIOLATIONS DE DONNÉES

AITRPRO notifie au Client toute violation de données à caractère personnel **sans retard injustifié** après en avoir pris connaissance et, dans la mesure du possible, dans un **délai maximal de 48 heures**.

Cette notification est accompagnée de toute documentation utile afin de permettre au Client de notifier cette violation à la CNIL (art. 33 RGPD). Elle contient au moins : la nature de la violation, les catégories et le nombre approximatif d'enregistrements/personnes concernés, le point de contact technique chez AITRPRO, les conséquences probables, et les mesures correctives prises ou proposées.

ARTICLE 6 – SOUS-TRAITEMENT ULTÉRIEUR

Le Client autorise AITRPRO à faire appel à des sous-traitants ultérieurs (hébergeurs cloud, opérateurs télécoms, éditeurs SaaS) pour mener à bien des activités de traitement spécifiques. AITRPRO tient à disposition du Client la liste à jour de ses sous-traitants ultérieurs.

AITRPRO s'assure par contrat que le sous-traitant ultérieur respecte les mêmes obligations de protection des données que celles fixées au présent DPA. **AITRPRO demeure pleinement responsable** devant le Client de l'exécution par le sous-traitant ultérieur de ses obligations. Tout ajout ou remplacement d'un sous-traitant sera notifié au Client, qui disposera de 15 jours pour émettre une objection légitime.

ARTICLE 7 – TRANSFERTS HORS UE

AITRPRO ne réalise ni n'autorise de transfert de données personnelles vers un pays situé hors de l'Espace économique européen (EEE), sauf sur instruction documentée du Client ou lorsque ce transfert est strictement nécessaire à l'exécution d'un service cloud souscrit par celui-ci (ex: Microsoft 365). Dans ce cas, AITRPRO s'assure que le transfert est encadré par un mécanisme juridiquement valable au titre du **Chapitre V du RGPD** (Décision d'adéquation, Clauses Contractuelles Types de la Commission Européenne).

ARTICLE 8 – SORT DES DONNÉES EN FIN DE CONTRAT

Au terme des prestations, ou en cas de résiliation du contrat, AITRPRO s'engage, au choix du Client :

- Soit à détruire toutes les données à caractère personnel ;
- Soit à les restituer au Client selon un format standard du marché.

Les copies résiduelles existantes dans les systèmes de sauvegarde d'AITRPRO sont isolées, non utilisées à des fins opérationnelles, et seront **supprimées automatiquement à l'expiration de leur durée de rétention**, sauf lorsqu'une disposition légale ou réglementaire applicable impose leur conservation.

ARTICLE 9 – DROIT D'AUDIT

AITRPRO met à la disposition du Client toutes les informations nécessaires pour démontrer le respect de ses obligations (art. 28 RGPD). Le Client peut réaliser un audit, à ses frais, une fois par an maximum, moyennant un préavis d'au moins 30 jours ouvrés.

Exception : Ces limitations de fréquence et de préavis ne s'appliquent pas en cas de violation de données personnelles avérée, de suspicion raisonnable de manquement substantiel, de demande d'une autorité de contrôle (CNIL), ou lorsque la réglementation l'impose.

L'audit ne pourra compromettre la sécurité, la confidentialité des données des autres clients d'AITRPRO, ni l'intégrité de ses environnements de production mutualisés.

ANNEXE 1 : DESCRIPTION DES TRAITEMENTS DE DONNÉES

Nature et Finalité du Traitement	Administration technique, télémaintenance, hébergement, supervision proactive, gestion des sauvegardes managées, sécurité du SI du Client (incluant la messagerie, les annuaires Active Directory, et la téléphonie VoIP) et support utilisateur (Helpdesk).
Catégories de Personnes concernées	Salariés, dirigeants, collaborateurs, partenaires, clients ou fournisseurs du Responsable de traitement dont les données transitent ou sont stockées de façon inhérente sur les infrastructures infogérées par AITRPRO.
Catégories de Données	Données d'identification (nom, prénom, login), coordonnées professionnelles (email, téléphone VoIP), données de connexion et logs techniques (adresses IP, horodatage, journaux <i>AI Sentinel</i>), et l'ensemble du contenu brut stocké par le Client sur ses serveurs/postes/cloud (fichiers, bases de données, courriels).
Durée du Traitement	Le traitement est réalisé pendant toute la durée d'exécution des prestations contractuelles (contrat d'infogérance, abonnements), majorée de la durée de rétention des routines de sauvegarde définies avec le Client.

ANNEXE 2 : MESURES TECHNIQUES ET ORGANISATIONNELLES (TOMS) D'AITRPRO

Conformément à l'Article 32 du RGPD, AITRPRO met en œuvre, en sa qualité de prestataire d'infogérance et de cybersécurité, les mesures suivantes pour garantir la sécurité et la confidentialité des données traitées pour le compte de ses Clients :

Contrôle des Accès Logiques (Habilitations)	• Application du principe de moindre privilège pour les techniciens AITRPRO. • Authentification forte (MFA - Multi-Factor Authentication) imposée sur l'ensemble des consoles d'administration, accès distants (VPN) et outils de supervision. • Gestion stricte et individuelle des mots de passe (utilisation de coffres-forts type KeePass/Bitwarden).
Sécurité des Communications et Chiffrement	• Chiffrement systématique des flux d'administration (SSH, HTTPS, VPN IPsec/SSL). • Déploiement de firewalls périmétriques matériels de nouvelle génération (NGFW WatchGuard) pour filtrer les accès non autorisés. • Chiffrement des données en transit et, lorsque techniquement applicable et validé par le Client, chiffrement des données au repos (ex: BitLocker sur les postes).
Traçabilité et Supervision (Logs)	• Journalisation des accès administrateurs et des événements de sécurité. • Utilisation de la suite propriétaire AI Sentinel et d'outils de monitoring (Zabbix, Checkmk) pour la supervision proactive, l'alerte précoce en cas de comportement suspect et la détection d'intrusions.
Sauvegarde, Résilience et Continuité (PCA/PRA)	• Architecture haute disponibilité sur les infrastructures d'hébergement critiques (Clusters Proxmox VE, stockage réparti Ceph). • Mise en œuvre de politiques de sauvegarde automatisées (Proxmox Backup Server, agents de sauvegarde externalisée) avec isolation des dépôts de sauvegarde pour résister aux ransomwares.
Sécurité Physique	• Accès sécurisés aux locaux d'AITRPRO (alarmes, serrures). • Hébergement des serveurs physiques chez des prestataires Datacenter certifiés (ISO 27001, contrôles d'accès biométriques, gardiennage 24/7).

Pour le Sous-traitant : AITRPRO
Patrice LESTIENNE, Gérant
DPA applicable à compter de sa version 1.1

Pour le Responsable de traitement (Client) :
L'acceptation du devis / contrat d'infogérance par le Client emporte adhésion pleine et entière aux présentes conditions de sous-traitance des données.