Accord de traitement des données (DPA) – Xylao

Apilice – Dernière mise à jour : 26 octobre 2026

Ce DPA encadre le traitement de données personnelles réalisé par Apilice pour ses clients via le logiciel Xylao, conformément à l'article 28 du RGPD.

Parties et préambule

Le sous-traitant : Apilice, SAS au capital de 150 €, SIREN 850 587 460, RCS Pontoise, siège social 19 rue du Buisson Flocourt, 95470 Saint-Witz, représentée par Patrick JOYEUX, Président. Contact données personnelles : contact@xylao.fr.

Le responsable de traitement : la société cliente de Xylao, identifiée lors de la création de son compte ou dans son bon de commande (« le Client »).

Le présent accord (« le DPA ») est annexé aux conditions générales d'utilisation de Xylao et en fait partie intégrante. Il prend effet à l'acceptation de ces conditions par le Client. En cas de contradiction sur la protection des données personnelles, le DPA prévaut.

Définitions. Les termes « données personnelles », « traitement », « responsable de traitement », « sous-traitant », « violation de données » et « personne concernée » ont le sens que leur donne le règlement (UE) 2016/679 (« RGPD »). « Xylao » désigne le logiciel édité par Apilice et mis à disposition du Client.

Article 1 – Objet, durée, nature et finalité

Apilice traite des données personnelles pour le compte du Client, uniquement pour fournir Xylao, plateforme de gestion des comptes rendus d'activité (CRA), dans les conditions prévues au contrat principal.

- Nature du traitement : hébergement, stockage, consultation, affichage et suppression des données saisies ou importées par le Client et ses utilisateurs.
- Finalité : fourniture, maintenance, support et sécurisation de Xylao.
- Durée : celle du contrat principal, prolongée du temps nécessaire à la restitution ou à la suppression des données (article 10).

Apilice n'utilise pas les données du Client pour son propre compte, ni à des fins commerciales ou d'entraînement de modèles.

Article 2 – Données et personnes concernées

Les catégories de données et de personnes concernées sont décrites en Annexe 1. Le Client reste responsable de déterminer les données qu'il saisit dans Xylao et de leur licéité (base légale, information des personnes, minimisation).

Le Client s'interdit de saisir dans Xylao des catégories particulières de données (article 9 du RGPD) ou des données relatives à des condamnations pénales (article 10), sauf accord écrit préalable d'Apilice.

Article 3 – Obligations d'Apilice

Apilice s'engage à :

- traiter les données uniquement sur instruction documentée du Client, le contrat principal et le DPA constituant ces instructions, y compris pour les transferts hors Union européenne ;
- informer immédiatement le Client si une instruction lui paraît contraire au RGPD ou à une autre disposition de protection des données ;
- garantir que les personnes autorisées à traiter les données sont tenues à une obligation de confidentialité, contractuelle ou légale ;
- appliquer les principes de protection des données dès la conception et par défaut ;
- aider le Client à respecter ses obligations relatives à l'analyse d'impact (articles 35 et 36 du RGPD), dans la limite des informations dont Apilice dispose ;
- tenir un registre des catégories d'activités de traitement effectuées pour le compte du Client (article 30.2 du RGPD) ;
- mettre à disposition du Client les informations nécessaires pour démontrer le respect du présent article.

Article 4 – Sécurité

Apilice met en œuvre les mesures techniques et organisationnelles décrites en Annexe 2, adaptées au risque (article 32 du RGPD). Elles incluent notamment le chiffrement des communications, le contrôle des accès par habilitation, la journalisation, des sauvegardes et la procédure de gestion des violations.

Apilice peut faire évoluer ces mesures, à condition de ne pas diminuer le niveau global de sécurité.

Article 5 – Sous-traitants ultérieurs

Le Client donne à Apilice une autorisation générale de recourir aux sous-traitants ultérieurs listés en Annexe 3.

Apilice informe le Client par écrit de tout ajout ou remplacement au moins 30 jours avant sa mise en œuvre. Le Client peut s'y opposer pour un motif raisonnable lié à la protection des données dans un délai de 15 jours. Si les parties ne trouvent pas de solution, le Client peut résilier le service concerné sans pénalité.

Apilice impose à chaque sous-traitant ultérieur, par contrat, des obligations de protection équivalentes à celles du DPA et reste responsable envers le Client de leur exécution.

Article 6 – Droits des personnes concernées

Le Client reste seul interlocuteur des personnes concernées. Si Apilice reçoit directement une demande d'exercice de droits (accès, rectification, effacement, limitation, portabilité, opposition), elle la transmet au Client sous 5 jours ouvrés, sans y répondre elle-même sauf instruction contraire.

Apilice aide le Client, par des mesures techniques et organisationnelles appropriées, à répondre à ces demandes. Les fonctionnalités d'export et de suppression de Xylao sont les moyens prévus à cet effet. Une assistance dépassant l'usage normal du logiciel peut être facturée sur devis.

Article 7 – Violations de données

Apilice notifie le Client par e-mail, dans les meilleurs délais et au plus tard 48 heures après en avoir pris connaissance, de toute violation de données personnelles affectant les données du Client.

La notification décrit, dans la mesure des informations disponibles : la nature de la violation, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, les conséquences probables et les mesures prises ou proposées. Apilice complète ces informations au fur et à mesure et aide le Client à notifier la CNIL (72 heures, article 33 du RGPD) et, le cas échéant, les personnes concernées (article 34).

Apilice consigne chaque violation dans un registre interne, avec ses conséquences et les mesures prises.

Article 8 – Localisation et transferts hors Union européenne

Les données du Client sont hébergées en France, chez OVH SAS (centre de données de Gravelines), sur un serveur privé virtuel (VPS) avec option de sauvegarde. Les sauvegardes sont également stockées en France.

Apilice ne transfère pas de données hors de l'Espace économique européen sans l'accord écrit du Client, sauf obligation légale. Le canal WhatsApp, facultatif et activé à la demande, fait appel à Meta Platforms Ireland Limited, qui peut transférer des données hors Union européenne dans le cadre des clauses contractuelles types de la Commission européenne ou du Data Privacy Framework. Ces traitements sont indiqués en Annexe 3.

Article 9 – Audit et preuves de conformité

Apilice met à disposition du Client la documentation nécessaire pour démontrer sa conformité : description des mesures de sécurité, liste à jour des sous-traitants ultérieurs, attestations ou certifications éventuelles.

Le Client peut réaliser, ou faire réaliser par un tiers tenu au secret, un audit au plus une fois par an, sur préavis écrit de 30 jours, pendant les heures ouvrées et sans perturber l'activité d'Apilice. Un audit supplémentaire est possible après une violation de données avérée. Les frais d'audit sont à la charge du Client.

Article 10 – Sort des données en fin de contrat

À la fin du contrat, le Client dispose de 30 jours pour récupérer ses données dans un format structuré et couramment utilisé, sur demande adressée à contact@xylao.fr. Passé ce délai, Apilice supprime les données de la base de production, sauf conservation exigée par la loi, et confirme la suppression par écrit sur demande.

Les copies de sauvegarde sont purgées selon leur cycle normal (sauvegardes quotidiennes conservées 14 jours), sous 90 jours maximum à compter de la fin du contrat.

Article 11 – Responsabilité, droit applicable

La responsabilité d'Apilice au titre du DPA est soumise aux limitations prévues au contrat principal, sans préjudice des dispositions impératives du RGPD (article 82).

Le DPA est régi par le droit français. Tout litige relève du tribunal compétent du ressort du siège d'Apilice (Pontoise), sauf disposition impérative contraire.

Annexe 1 – Description du traitement

Élément	Description
Personnes concernées	Utilisateurs du Client (administrateurs, collaborateurs, signataires), prestataires indépendants et collaborateurs de fournisseurs rattachés au Client, contacts des sociétés partenaires.
Données traitées	Identité et coordonnées professionnelles (nom, prénom, e-mail, téléphone), mot de passe et codes de vérification (hachés), journaux de connexion (date, adresse IP, résultat), comptes rendus d'activité (périodes, volumes d'heures ou de jours, observations), relations entre sociétés, historique et signatures horodatées des CRA, invitations.
Données sensibles	Aucune.
Finalité	Fourniture du logiciel Xylao.
Durée de conservation	Durée du contrat. Après la fin du contrat : suppression de la base de production sous 30 jours et des sauvegardes sous 90 jours (article 10). Journaux de connexion : 12 mois glissants.

Annexe 2 – Mesures de sécurité

- Chiffrement des échanges : communications chiffrées via HTTPS ; sauvegardes chiffrées.
- Authentification : double authentification à chaque connexion (code à usage unique par e-mail, SMS ou WhatsApp) ; mots de passe hachés avec scrypt, codes de vérification hachés ; verrouillage du compte après 5 échecs en 15 minutes ; sessions HTTP-only expirant après 1 heure.
- Gestion des droits par profil (administrateur, standard, lecture).
- Séparation logique stricte des données entre sociétés (cloisonnement multi-tenant) à chaque écran et chaque requête.
- Accès à la base de données limité au strict nécessaire : le compte applicatif ne peut qu'exécuter des procédures stockées.
- Accès administrateur aux serveurs réservé à l'hyperviseur Apilice.
- Journalisation des connexions et des actions d'administration ; piste d'audit de chaque CRA (soumission, validation, refus, signature horodatée).
- Sauvegardes : quotidiennes, conservées 14 jours, stockées en France.
- Hébergement en France, centre de données de Gravelines.
- Procédure de gestion des violations de données : détection et confinement, évaluation, information du Client sous 48 heures, notification CNIL sous 72 heures, registre des violations.

Annexe 3 – Sous-traitants ultérieurs

Sous-traitant	Service rendu	Localisation du traitement	Garantie de transfert hors UE
OVH SAS	Hébergement du serveur et de la base de données	France (Gravelines)	Sans objet
OVH (smtp.mail.ovh.net)	Envoi d'e-mails transactionnels (codes, invitations, rappels)	France	Sans objet
allMySMS	Envoi de SMS transactionnels (codes de vérification, relances)	France	Sans objet

Meta Platforms Ireland Limited (WhatsApp Business)	Envoi de messages WhatsApp (codes, relances), uniquement si ce canal est activé	Irlande (UE) ; transferts possibles hors UE	Clauses contractuelles types ou Data Privacy Framework
GoCardless SAS	Prélèvement SEPA de l'abonnement (mandat et paiements)	France ; traitements pouvant impliquer le Royaume-Uni	Décision d'adéquation de la Commission européenne
WeInvoice	Émission des factures électroniques de l'abonnement	France	Sans objet