Accord de traitement des données (DPA)

Version 1.2 — 25 juillet 2026 (remplace la version 1.1 du 10 juin 2026)

Conformément à l'article 28 du Règlement (UE) 2016/679 (« RGPD »).

Préambule

Le présent Accord de traitement des données (« DPA ») encadre le traitement des données à caractère personnel effectué par le Sous-traitant pour le compte du Responsable de traitement, dans le cadre de l'utilisation du service conv2pdf (conversion de fichiers depuis et vers le format PDF, accessible via interface web et API REST sur les domaines `conv2pdf.com` et `api.conv2pdf.com`).

Il complète les Conditions Générales de Vente et le contrat d'abonnement souscrit par le Responsable de traitement. En cas de contradiction entre le présent DPA et les CGV, le DPA prévaut pour ce qui concerne le traitement des données à caractère personnel.

1. Identification des parties

1.1 Le Sous-traitant

- **Nom commercial :** Iris Digital
- **Représentant :** Jamal Tantaoui
- **Forme juridique :** Entreprise Individuelle (régime micro-entrepreneur)
- **SIREN :** 524 317 872
- **Siège social :** 8 chemin dou Sarpout, 33610 Cestas, France
- **Contact :** contact@conv2pdf.com

Ci-après désigné « **conv2pdf** » ou le « Sous-traitant ».

1.2 Le Responsable de traitement

Toute personne physique ou morale ayant souscrit un abonnement payant à l'API conv2pdf (plans Starter, Growth, Business, Enterprise) ou utilisant le service en mode B2B sous compte authentifié. Identifié au moment de la signature du présent DPA par :

- dénomination sociale ou nom ;
- forme juridique ;
- numéro d'immatriculation ;
- adresse du siège ;
- représentant signataire et fonction ;
- email professionnel de contact.

Ci-après désigné le « Responsable de traitement » ou le « Client ».

2. Définitions

Les termes en majuscule non définis ci-dessous ont le sens qui leur est donné par le RGPD.

- **Données à caractère personnel :** toute information se rapportant à une personne physique identifiée ou identifiable, telle que définie à l'article 4 du RGPD.
- **Traitement :** toute opération effectuée sur des Données à caractère personnel, au sens de l'article 4 du RGPD.
- **Responsable de traitement :** le Client, qui détermine les finalités et les moyens du Traitement.
- **Sous-traitant :** conv2pdf, qui traite les Données pour le compte du Responsable de traitement.
- **Sous-traitants ultérieurs :** les prestataires auxquels conv2pdf fait appel pour exécuter le service (cf. Annexe 2).
- **Personne concernée :** la personne physique dont les Données sont traitées.
- **Violation de données :** une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données ou l'accès non autorisé à de telles Données.

3. Objet, nature et finalité du Traitement

3.1 Objet

Le Sous-traitant traite, pour le compte du Responsable de traitement, les Données contenues dans les fichiers téléversés via l'API ou l'interface web conv2pdf, aux seules fins de conversion depuis et vers le format PDF (et opérations associées : fusion, division, compression, protection par mot de passe, partage public).

3.2 Nature du Traitement

Les opérations couvertes par le présent DPA sont :

- la réception et le stockage temporaire du fichier d'entrée ;
- la conversion automatisée depuis et vers le format PDF par les outils libres LibreOffice, Ghostscript, qpdf, sharp, pdf-lib, pdf2docx et PyMuPDF ;
- la mise à disposition du fichier de sortie au Responsable de traitement ;
- la suppression automatique des fichiers d'entrée et de sortie au plus tard une heure après leur création, à l'exception du fichier mis à disposition par un lien de partage généré par le Responsable de traitement, conservé jusqu'à l'échéance que celui-ci a fixée (au maximum sept jours en offre Gratuite, trente jours en offre Premium) ou jusqu'à sa révocation ;
- la journalisation technique (horodatage, outil utilisé, nom du fichier d'origine, taille, durée, statut) à des fins statistiques et de facturation.

3.3 Finalité

Exécution du contrat de service de conversion PDF souscrit par le Responsable de traitement (article 6.1.b du RGPD).

3.4 Durée

Le présent DPA prend effet à la date d'acceptation par le Responsable de traitement et reste en vigueur pendant toute la durée de l'abonnement à l'API conv2pdf. Il prend fin de plein droit à la résiliation de l'abonnement, sans préjudice des obligations qui survivent au terme du contrat (notamment la suppression des Données).

3.5 Catégories de Données traitées et de Personnes concernées

Cf. **Annexe 3**.

4. Obligations du Sous-traitant

4.1 Traitement sur instructions documentées

Le Sous-traitant ne traite les Données que sur instructions documentées du Responsable de traitement, y compris en ce qui concerne les transferts vers un pays tiers, sauf obligation légale contraire. Les instructions documentées résultent du présent DPA, des CGV et des paramètres explicites passés aux endpoints de l'API.

4.2 Confidentialité

Le Sous-traitant veille à ce que les personnes autorisées à traiter les Données s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

4.3 Mesures de sécurité

Le Sous-traitant met en œuvre les mesures techniques et organisationnelles décrites en **Annexe 1**, conformément à l'article 32 du RGPD.

4.4 Sous-traitants ultérieurs

Le Responsable de traitement autorise le Sous-traitant à faire appel aux sous-traitants ultérieurs listés en **Annexe 2**. Toute modification de cette liste (ajout, remplacement) sera notifiée au Responsable de traitement par email avec un préavis d'au moins trente jours, durant lequel le Responsable de traitement peut formuler une objection motivée. À défaut d'objection dans ce délai, la modification est réputée acceptée.

Le Sous-traitant impose à chaque sous-traitant ultérieur les mêmes obligations en matière de protection des Données que celles prévues au présent DPA, par contrat écrit.

4.5 Assistance au Responsable de traitement

Le Sous-traitant assiste le Responsable de traitement, par des mesures techniques et organisationnelles appropriées et dans la mesure du possible, pour :

- répondre aux demandes d'exercice des droits des Personnes concernées (accès, rectification, effacement, opposition, portabilité, limitation) ;
- garantir le respect des obligations prévues aux articles 32 à 36 du RGPD (sécurité, notification, analyse d'impact, consultation préalable).

4.6 Notification d'une Violation de données

En cas de Violation de données concernant les Données traitées pour le compte du Responsable de traitement, le Sous-traitant la notifie au Responsable de traitement dans les meilleurs délais et au plus tard dans les soixante-douze heures après en avoir pris connaissance, par email à l'adresse de contact renseignée au compte client.

La notification précise au minimum :

- la nature de la Violation, y compris les catégories et le nombre approximatif de Personnes concernées et d'enregistrements de Données concernés ;

- les conséquences probables ;
- les mesures prises ou proposées pour remédier à la Violation et atténuer ses effets.

4.7 Suppression ou restitution des Données

Au terme du présent DPA, et au choix du Responsable de traitement formulé par écrit dans les trente jours suivant la résiliation, le Sous-traitant procède :

- soit à la suppression définitive de toutes les Données traitées pour le compte du Responsable de traitement, y compris les copies de sauvegarde, dans un délai maximum de soixante jours ;
- soit à la restitution de ces Données au Responsable de traitement sous format standard et lisible par machine, puis à leur suppression.

À défaut de demande dans le délai de trente jours, le Sous-traitant procède automatiquement à la suppression. La compression et l'effacement des sauvegardes peuvent prendre jusqu'à soixante jours supplémentaires en raison du cycle naturel de rotation des backups (cf. Annexe 1).

4.8 Audit

Le Sous-traitant met à la disposition du Responsable de traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent DPA. Il permet la réalisation d'audits par le Responsable de traitement ou par un auditeur indépendant mandaté par lui, dans la limite d'un audit par année civile, sur rendez-vous fixé au moins trente jours à l'avance, sans préjudice du droit de la CNIL ou de toute autorité de contrôle compétente.

5. Obligations du Responsable de traitement

Le Responsable de traitement :

- s'assure de disposer d'une base légale appropriée pour le Traitement des Données qu'il soumet au Sous-traitant ;
- informe les Personnes concernées du recours au Sous-traitant et de la nature du Traitement ;
- garantit que les Données soumises sont licites, exactes et limitées à ce qui est nécessaire à la finalité poursuivie ;
- ne soumet pas, via le service, de catégories particulières de Données (article 9 du RGPD) ou de Données relatives à des condamnations pénales (article 10) sans avoir préalablement informé le Sous-traitant et obtenu son accord écrit.

6. Transferts hors Union européenne

Le Sous-traitant garantit qu'**aucun transfert** de Données vers un pays tiers ou une organisation internationale hors Union européenne n'a lieu dans le cadre du service conv2pdf. L'ensemble de l'infrastructure (serveurs, bases de données, sauvegardes, email transactionnel) est situé en France ou dans l'Union européenne (cf. Annexe 2).

Stripe Payments Europe Ltd, basée en Irlande, est seule susceptible d'utiliser, pour des opérations de prévention de la fraude, des composants techniques situés hors UE ; toutefois, aucune Donnée contenue dans les fichiers convertis n'est transmise à Stripe (Stripe ne reçoit que les informations de paiement et l'email de facturation).

7. Durée, résiliation et survie

Le présent DPA suit le sort du contrat d'abonnement. Les obligations relatives à la confidentialité (article 4.2), à la suppression des Données (article 4.7) et à la notification rétroactive d'une Violation de données antérieure (article 4.6) survivent à la résiliation pour la durée nécessaire à leur exécution.

8. Droit applicable et juridiction

Le présent DPA est régi par le droit français. Tout litige relatif à son interprétation ou à son exécution relève de la compétence exclusive des tribunaux du ressort du siège du Sous-traitant, sauf disposition légale impérative contraire.

9. Signatures

Le Sous-traitant	Le Responsable de traitement
Jamal Tantaoui	*Nom du signataire*
Représentant de Iris Digital	*Fonction*
Date : _____	Date : _____
Signature :	Signature :

Annexe 1 — Mesures techniques et organisationnelles (TOMs)

Conformément à l'article 32 du RGPD, le Sous-traitant met en œuvre les mesures suivantes.

A1.1 Sécurité du transport

- Chiffrement TLS 1.2 minimum (TLS 1.3 supporté) sur l'ensemble des connexions HTTPS, certificats Let's Encrypt renouvelés automatiquement.
- Redirection automatique HTTP vers HTTPS, en-tête HSTS d'un an avec inclusion des sous-domaines.

A1.2 Sécurité du stockage

- Fichiers d'entrée et de sortie supprimés au plus tard une heure après création (suppression automatisée par cron interne s'exécutant toutes les cinq minutes). Seule exception : le fichier copié dans le magasin de partage lorsque le Responsable de traitement génère un lien de partage, supprimé à l'échéance du lien ou à sa révocation.
- Aucun cache résultat : deux conversions du même fichier produisent deux PDF strictement indépendants, stockés et purgés séparément.
- Mots de passe (le cas échéant) hachés avec Argon2id, jamais stockés en clair.
- Clés API hachées en SHA-256, jamais stockées en clair, affichées une seule fois lors de leur création.
- Cookies de session signés HMAC, attribut HttpOnly, SameSite Lax, durée de vie de trente jours.

A1.3 Sécurité réseau

- Protection anti-DDoS L3/L4 incluse par l'hébergeur OVH.
- Limitation de débit applicative par adresse IP (Nginx + module rate-limit).
- Pare-feu UFW configuré en deny par défaut, ouvertures uniquement sur 80/443 et un port SSH personnalisé.
- Bannissement automatique par fail2ban en cas de tentatives répétées (login, accès à des fichiers protégés par mot de passe).
- Détection d'intrusion par rkhunter.

A1.4 Sécurité des accès administratifs

- SSH limité à des adresses IP en liste blanche, sur un port non standard.
- Authentification par clé Ed25519 uniquement, mot de passe désactivé.
- Compte applicatif distinct du compte d'administration, sans accès SSH entrant.
- Service applicatif lancé sous systemd avec contraintes de sécurité (NoNewPrivileges, ProtectHome, ProtectSystem strict, namespaces restreints).

A1.5 Journalisation et traçabilité

- Logs serveur Nginx conservés quatorze jours pour la sécurité.
- Métadonnées techniques des conversions (outil utilisé, nom du fichier d'origine, taille, durée, statut) conservées trente jours à des fins statistiques.
- En cas d'utilisation de la fonctionnalité de partage public, adresse IP, port source et user-agent du contributeur sont conservés un an dans un journal d'audit dédié, conformément à l'article 6 II de la loi pour la confiance dans l'économie numérique et au décret n° 2021-1363. Ces données ne sont communiquées qu'à l'autorité judiciaire sur réquisition formelle.

A1.6 Sauvegardes

- Sauvegardes automatiques des bases de données toutes les six heures, chiffrées en transit (TLS) vers un stockage objet OVH situé en France (Strasbourg).
- Rétention de quatorze jours en local et trente jours en stockage objet, suppression automatisée des sauvegardes plus anciennes.

A1.7 Mises à jour et maintenance

- Système d'exploitation Debian stable, mises à jour de sécurité installées dans un délai maximum de trente jours après publication par l'éditeur.
- Dépendances applicatives suivies via Dependabot avec montée de version mineure et de sécurité automatique, revue manuelle pour les changements majeurs.

A1.8 Confidentialité du personnel

- Le Sous-traitant est une entreprise individuelle ; aucun salarié n'a accès aux Données. Le représentant légal est lui-même soumis à une obligation de confidentialité au titre du présent DPA.

- En cas de recours futur à des collaborateurs ou prestataires, ceux-ci seront contractuellement soumis à une obligation de confidentialité équivalente avant tout accès aux Données.

Annexe 2 — Sous-traitants ultérieurs autorisés

Sous-traitant ultérieur	Pays	Rôle	Données transmises
OVH SAS	France (Roubaix, datacenter Gravelines)	Hébergement infrastructure	Ensemble des Données, en environnement chiffré
Brevo	France	Emails transactionnels (lien magique de connexion, vérification de changement d'email, transfert des messages du formulaire de contact)	Email du destinataire, contenu de l'email
Stripe Payments Europe Ltd	Irlande	Traitement des paiements (abonnements Premium et API payants)	Email professionnel du client, identifiant client Stripe, montants. **Stripe ne reçoit aucune Donnée contenue dans les fichiers convertis.**

Aucun de ces sous-traitants ultérieurs n'est situé hors Union européenne au sens du RGPD.

Annexe 3 — Catégories de Données et de Personnes concernées

A3.1 Données traitées

Le Sous-traitant traite les Données à caractère personnel suivantes :

- contenu des fichiers téléversés par le Client ou par les utilisateurs finaux du Client, lorsque ces fichiers contiennent des Données à caractère personnel (le contenu n'est jamais inspecté, indexé ou analysé) ;
- adresse email du compte API du Client ;
- adresses IP des requêtes API et des accès à l'interface web ;
- identifiant client Stripe (pour la facturation) ;
- métadonnées techniques des conversions (horodatage, outil utilisé, nom du fichier d'origine, taille, durée, statut).

A3.2 Personnes concernées

- le Client de l'API (personne physique souscrivant l'abonnement, ou personne physique représentant la personne morale Client) ;
- les utilisateurs finaux du Client lorsqu'ils interagissent indirectement avec conv2pdf via l'intégration du Client ;
- les personnes dont les Données figurent dans les fichiers convertis, dont la nature dépend de l'usage que le Client fait du service.

A3.3 Durée de conservation

Donnée	Durée	Motif
Fichier d'entrée et fichier converti	1 heure maximum	Exécution du service
Fichier mis à disposition par lien de partage	7 jours (Gratuit) / 30 jours (Premium) maximum, ou jusqu'à révocation	Exécution du service, à l'initiative du Responsable de traitement
Métadonnées job (outil, nom du fichier d'origine, taille, durée, statut)	30 jours	Statistiques internes et facturation
Compte client (email, plan, clés API hachées)	Durée de l'abonnement	Exécution du contrat
Identifiant client Stripe	10 ans	Obligation légale comptable
Logs serveur Nginx	14 jours	Sécurité
Journal d'audit des partages publics (IP, port, user-agent)	1 an	Obligation légale LCEN
Sauvegardes des bases de données	14 jours local / 30 jours stockage objet	Continuité de service

---

En cas de divergence entre la présente version française et toute traduction, la version française fait foi.