PALLADIUM COOKIES

Accord de sous-traitance — Art. 28 RGPD

Modèle public · à compléter avant signature commerciale

Préambule

Le présent Accord de sous-traitance (« DPA ») encadre le traitement de données à caractère personnel effectué par Palladium Cookies (le « Sous-traitant ») pour le compte du Client (le « Responsable de traitement ») dans le cadre de la fourniture de la plateforme Palladium Cookies (le « Service »). Il complète le contrat principal (Conditions Générales d'Utilisation ou contrat commercial spécifique).

1. Parties

Le Sous-traitant : Palladium Cookies, plateforme SaaS de gestion du consentement, joignable à legal@palladium.cookies. Le Responsable de traitement : la personne morale identifiée dans le contrat principal. Les Parties reconnaissent que le présent DPA s'inscrit dans la qualification de traitement définie aux articles 4(7) et 4(8) du RGPD.

2. Objet, durée, nature et finalités

Objet : fourniture du Service et traitement des données nécessaires à son fonctionnement.

Durée : celle du contrat principal et toute période postérieure nécessaire à la restitution ou suppression des données.

Nature : collecte, enregistrement, conservation, consultation, communication par transmission, rapprochement, restriction, effacement.

Finalités : gestion du consentement des visiteurs du site web du Responsable de traitement, production des preuves de consentement art. 30, mise à disposition des outils d'administration et d'audit.

3. Catégories de données et de personnes concernées

Personnes concernées : visiteurs du site du Responsable de traitement, administrateurs et utilisateurs internes du Responsable de traitement disposant d'un accès à la console.

Catégories de données : identifiants techniques de session, identifiant de consentement pseudonymisé, horodatage UTC, version de bannière et de politique acceptée, finalités acceptées ou refusées, hash SHA-256 de l'adresse IP, géolocalisation grossière (pays, ville). Aucun nom, prénom, email, ni adresse IP en clair de visiteur final n'est conservé par le Sous-traitant.

4. Obligations du Sous-traitant

- Traiter les données uniquement sur instruction documentée du Responsable de traitement (art. 28(3)(a) RGPD).
- Garantir la confidentialité des personnes autorisées à accéder aux données (art. 28(3)(b) RGPD).

- Mettre en œuvre les mesures techniques et organisationnelles appropriées (art. 32 RGPD), précisées en Annexe sécurité.
- Aider le Responsable de traitement à répondre aux demandes des personnes concernées (art. 12-22 RGPD).
- Notifier au Responsable de traitement toute violation de données dans un délai de 72 heures suivant sa découverte (art. 33 RGPD).
- Restituer ou supprimer les données à la fin du contrat, au choix du Responsable de traitement (art. 28(3)(g) RGPD).
- Mettre à disposition toutes les informations nécessaires pour démontrer le respect des obligations art. 28.

5. Sous-traitants ultérieurs

Le Responsable de traitement autorise le recours à des sous-traitants ultérieurs sous réserve d'une notification préalable de 30 jours avant tout ajout, et du droit d'opposition motivé. La liste à jour des sous-traitants ultérieurs est publiée à palladium.cookies/legal/subprocessors et notifiée par email aux administrateurs des comptes concernés.

6. Transferts hors Union Européenne

Les données sont hébergées dans l'Union Européenne par défaut. Tout transfert hors UE est encadré par les Clauses Contractuelles Types de la Commission européenne (décision d'exécution UE 2021/914) et fait l'objet d'une analyse d'impact des transferts (Transfer Impact Assessment) documentée et tenue à disposition du Responsable de traitement sur demande.

7. Mesures techniques et organisationnelles

- Hébergement Union Européenne, fournisseur certifié ISO 27001 et SOC 2.
- Chiffrement TLS 1.3 en transit, AES-256 au repos sur les volumes et les sauvegardes.
- Authentification par identifiant + mot de passe (PBKDF2-HMAC-SHA256, 210 000 itérations, sel par utilisateur), MFA TOTP RFC 6238 optionnel, RBAC. SSO OpenID Connect en feuille de route.
- Sauvegardes chiffrées quotidiennes, rétention 30 jours, restauration testée régulièrement.
- Journaux structurés conservés 12 mois, corrélation centralisée, supervision continue.
- Filtrage anti-DDoS, limitation de débit, listes d'autorisation IP sur l'API d'administration.
- Cycle de développement sécurisé : revue de code, SAST, SCA, secrets gérés hors dépôt.

Accord de sous-traitance — Art. 28 RGPD

Modèle public · à compléter avant signature commerciale

8. Audit

Le Responsable de traitement peut auditer le respect du présent DPA, soit en s'appuyant sur les rapports d'audit indépendants fournis par le Sous-traitant (questionnaires VSAQ, SIG-Lite, CAIQ ; futurs rapports ISO 27001 et SOC 2), soit, dans les limites raisonnables, par audit sur site annoncé 30 jours à l'avance.

9. Notification d'incident

Tout incident de sécurité susceptible d'affecter les données personnelles fait l'objet d'une notification au Responsable de traitement dans un délai de 72 heures suivant sa découverte, comportant : la nature de l'incident, les catégories et le volume approximatif des données concernées, les conséquences probables, les mesures prises ou proposées pour remédier à la violation et atténuer ses effets éventuels.

10. Fin du contrat

À la fin du contrat principal, le Sous-traitant procède, au choix du Responsable de traitement et dans un délai de 30 jours, à la restitution des données dans un format structuré (CSV ou JSON) ou à leur suppression irréversible, y compris des sauvegardes, dans un délai supplémentaire de 90 jours.

Annexe — Liste des sous-traitants ultérieurs

Liste publique et tenue à jour à palladium.cookies/legal/subprocessors. Hébergement, CDN, email transactionnel, supervision, captures d'erreurs, paiement, support — tous sous-traitants identifiés avec leur juridiction, leur rôle et la nature des données traitées.

Pour signature

Demandez la version exécutable du DPA, intégrant vos coordonnées et toute clause spécifique, à legal@palladium.cookies. Une signature électronique avec horodatage qualifié est disponible.