Bureau de Protection Digitale
Aoufi Ventures LLC
BPD-LEG-02

Politique de confidentialité

Version du 20 novembre 2026

Le Bureau de Protection Digitale (BPD) est le nom commercial d'un service opéré par Aoufi Ventures LLC, société constituée dans l'État du Wyoming (États-Unis), immatriculée sous le numéro 2025-001698191. La présente politique décrit les données que nous traitons, les raisons de ce traitement, leurs destinataires, leur durée de conservation et la manière d'exercer vos droits. Elle s'applique conformément à la loi marocaine n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et, pour les personnes situées dans l'Union européenne, au Règlement (UE) 2016/679 (RGPD).

Article 1. Responsable du traitement

Lorsqu'un client fait appel directement au bureau, Aoufi Ventures LLC agit comme responsable du traitement des données nécessaires à la relation, à l'exécution de la mission, à la facturation et à la sécurité.

Lorsqu'une entreprise, un cabinet d'avocats ou un family office nous transmet des données concernant des personnes qu'il représente et détermine les finalités du traitement, il agit en général comme responsable du traitement et le bureau comme sous-traitant, dans le cadre d'un accord écrit. Le bureau reste responsable de ses propres traitements de facturation, de prévention de la fraude, de conformité et de sécurité.

Article 2. Données traitées

Données d'identification et de contact : nom, prénom, fonction, organisation, adresse électronique, numéro de téléphone.

Données relatives à la mission : secteur, marques, noms et comptes officiels à protéger, plateformes concernées, degré d'urgence, liens et éléments signalés, images de référence, preuves de titularité des droits, échanges avec le bureau. Les images de référence servent uniquement à retrouver leurs copies en ligne.

Données de vérification : lorsqu'une vérification d'identité ou de mandat est nécessaire, seuls les éléments utiles sont demandés. Le demandeur peut masquer les autres informations du document transmis.

Données techniques : adresse IP, type de navigateur, journaux de connexion de l'hébergeur du site.

Article 3. Informations issues de sources publiques

Pour fournir ses services de surveillance, le bureau peut collecter des adresses de pages, noms d'utilisateur, images, métadonnées et autres informations publiquement accessibles sur les sites, moteurs de recherche, réseaux sociaux, hébergeurs et plateformes désignés par le client. Ces

informations peuvent concerner le client, des personnes qui usurpent son identité ou d'autres personnes apparaissant dans les contenus signalés.

Lorsque la loi l'exige, le bureau fournit l'information prévue à l'article 14 du RGPD. Lorsque cette information est impossible, exigerait des efforts disproportionnés ou compromettrait gravement la finalité du traitement, notamment le retrait d'un contenu illicite, le bureau documente cette analyse et met en œuvre des garanties appropriées. Toute personne concernée peut s'opposer au traitement en écrivant à privacy@bureauprotectiondigitale.fr.

Article 4. Données sensibles

Certaines missions portent sur des images ou documents privés, y compris à caractère intime, ou sur des montages et contenus générés par intelligence artificielle reproduisant l'image ou la voix d'une personne. Ces données relèvent des catégories particulières au sens de l'article 9 du RGPD et des données sensibles au sens de la loi n° 09-08. Elles sont traitées sur la base du consentement explicite de la personne concernée ou lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice, et uniquement pour obtenir leur retrait.

Article 5. Finalités et bases légales

- Répondre à une demande et établir une proposition : mesures précontractuelles prises à la demande de la personne et consentement.
- Exécuter la mission (surveillance, constats, demandes de retrait, rapports) : exécution du contrat.
- Constater et signaler une usurpation ou une atteinte, et conserver les preuves : intérêt légitime du client à faire cesser l'atteinte et intérêt légitime du bureau à se défendre en cas de litige.
- Sécuriser les services et prévenir la fraude : intérêt légitime.
- Tenir la comptabilité et répondre aux obligations légales : obligation légale.

Article 6. Décisions automatisées

Le système utilisé par le bureau automatise la recherche et la documentation des contenus. Aucune décision produisant des effets juridiques ou affectant une personne de manière significative n'est prise sans examen humain : chaque demande de retrait est validée par un analyste.

Article 7. Destinataires

Les données ne sont jamais vendues. Elles sont communiquées uniquement :

- aux membres habilités du bureau, dans la limite de leurs fonctions ;
- aux prestataires techniques nécessaires au service : hébergement du site (Vercel), infrastructure Content Removal Desk (CRD), dont la base de données et le stockage sont situés dans l'Union européenne, réception des formulaires (Formspree), messagerie électronique et, à la demande du client, messagerie chiffrée Signal ;
- aux plateformes, hébergeurs, registraires et moteurs de recherche destinataires d'un signalement, pour les seules informations nécessaires à ce signalement ;
- aux avocats et conseils intervenant dans le dossier, avec l'accord du client ;
- aux autorités, lorsque la loi l'exige.

Les prestataires et partenaires sont tenus par des obligations de confidentialité et ne peuvent utiliser les données qu'aux fins prévues.

Article 8. Transferts hors du Maroc et de l'Union européenne

Certains prestataires sont établis aux États-Unis. Ces transferts sont encadrés par des clauses contractuelles types approuvées par la Commission européenne ou par le cadre de protection des données UE-États-Unis pour les prestataires certifiés, et réalisés conformément à la loi n° 09-08, y compris, lorsqu'elle est requise, l'autorisation de la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP).

Article 9. Sécurité

- Chiffrement des données au repos et en transit.
- Accès aux dossiers limité aux personnes habilitées.
- Sauvegardes chiffrées, conservées dans l'Union européenne.
- Examen humain de chaque action engagée au nom d'un client.

Article 10. Espace de suivi et intégrations

Lorsque la mission le prévoit, les équipes habilitées du client accèdent à un espace de suivi sécurisé ou à une interface de programmation (API). Les accès sont personnels et réservés aux utilisateurs désignés par le client ; les journaux de connexion sont conservés pour la durée indiquée ci-dessous.

Article 11. Violation de données

En cas de violation de données susceptible d'engendrer un risque pour les droits et libertés des personnes, le bureau notifie l'autorité compétente dans les délais légaux (72 heures au titre du RGPD) et informe les personnes concernées lorsque le risque est élevé, en précisant les mesures prises.

Article 12. Durées de conservation

- Demandes sans suite : 12 mois après le dernier échange.
- Données de mission : durée de la mission, puis 3 ans.
- Dossiers de preuves et demandes de retrait : 5 ans, pour la défense des droits.
- Documents de vérification : durée strictement nécessaire à la vérification ou à la procédure qui l'exige.
- Pièces comptables : durée légale applicable.
- Journaux techniques : 12 mois.

Au terme de ces durées, les données sont supprimées ou anonymisées de manière irréversible.

Article 13. Vos droits

Au titre de la loi n° 09-08, vous disposez d'un droit d'accès, de rectification et d'opposition pour des motifs légitimes. Si vous êtes situé dans l'Union européenne, vous disposez en outre des droits d'effacement, de limitation, de portabilité et du droit de retirer votre consentement à tout moment.

Pour exercer ces droits : privacy@bureauprotectiondigitale.fr. Une justification d’identité peut être demandée. Une réponse est apportée dans les délais légaux.

Article 14. Réclamation

- Maroc : Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), www.cndp.ma
- France : Commission nationale de l’informatique et des libertés (CNIL), www.cnil.fr
- Autres pays de l’Union européenne : autorité nationale de protection des données (liste sur edpb.europa.eu)

Article 15. Mineurs

Lorsqu’une situation concerne un mineur, la demande est présentée par son représentant légal.

Article 16. Modifications

La présente politique peut être modifiée. La version en vigueur et sa date figurent en tête du document.