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

Privacy policy

Version of 20 November 2026

The Bureau de Protection Digitale (BPD) is the trade name of a service operated by Aoufi Ventures LLC, a company formed in the State of Wyoming (United States), registration number 2025-001698191. This policy describes the data we process, why, who receives it, how long it is kept and how to exercise your rights. It applies in accordance with Moroccan Law No. 09-08 on the protection of individuals with regard to the processing of personal data and, for people located in the European Union, Regulation (EU) 2016/679 (GDPR).

Article 1. Data controller

When a client engages the office directly, Aoufi Ventures LLC acts as controller of the data needed for the relationship, the engagement, invoicing and security.

When a company, law firm or family office sends us data about people it represents and determines the purposes of processing, it generally acts as controller and the office as processor, under a written agreement. The office remains controller of its own invoicing, fraud prevention, compliance and security processing.

Article 2. Data processed

Identification and contact data: first and last name, position, organisation, email address, phone number.

Engagement data: sector, brands, names and official accounts to protect, platforms concerned, urgency level, reported links and items, reference images, proof of rights, correspondence with the office. Reference images are used only to find their copies online.

Verification data: when identity or authority must be verified, only the elements needed are requested. The requester may mask the other information on the document provided.

Technical data: IP address, browser type, connection logs of the website host.

Article 3. Information from public sources

To provide its monitoring services, the office may collect page addresses, usernames, images, metadata and other publicly accessible information from websites, search engines, social networks, hosts and platforms identified by the client. This may concern the client, people impersonating them or other people appearing in the reported content.

Where the law requires, the office provides the information set out in Article 14 GDPR. Where that information is impossible, would involve disproportionate effort or would seriously impair the purpose of the processing, in particular the removal of unlawful content, the office documents that assessment

and implements appropriate safeguards. Any person concerned may object by writing to privacy@bureauprotectiondigitale.fr.

Article 4. Sensitive data

Some engagements concern private images or documents, including intimate ones, or montages and AI-generated content reproducing a person's image or voice. These are special category data under Article 9 GDPR and sensitive data under Law No. 09-08. They are processed on the basis of the explicit consent of the person concerned, or where processing is necessary to establish, exercise or defend legal claims, and only to obtain their removal.

Article 5. Purposes and legal bases

- Answering a request and preparing a proposal: pre-contractual steps taken at the person's request, and consent.
- Carrying out the engagement (monitoring, evidence, removal requests, reports): performance of the contract.
- Recording and reporting impersonation or an infringement, and keeping evidence: the client's legitimate interest in stopping it and the office's legitimate interest in defending itself in a dispute.
- Securing the services and preventing fraud: legitimate interest.
- Keeping accounts and meeting legal obligations: legal obligation.

Article 6. Automated decisions

The system used by the office automates the search for and documentation of content. No decision with legal effects or that significantly affects a person is made without human review: every removal request is approved by an analyst.

Article 7. Recipients

Data is never sold. It is shared only with:

- authorised members of the office, within the scope of their duties;
- technical providers the service requires: website hosting (Vercel), the Content Removal Desk (CRD) infrastructure, whose database and storage are located in the European Union, form handling (Formspree), email and, at the client's request, Signal encrypted messaging;
- the platforms, hosts, registrars and search engines that receive a report, for the information that report requires and nothing more;
- lawyers and advisers working on the case, with the client's agreement;
- authorities, where the law requires it.

Providers and partners are bound by confidentiality obligations and may use the data only for the intended purposes.

Article 8. Transfers outside Morocco and the European Union

Some providers are based in the United States. These transfers are covered by standard contractual clauses approved by the European Commission or by the EU-US Data Privacy Framework for certified providers, and carried out in accordance with Law No. 09-08, including, where required, the authorisation of Morocco's data protection authority (CNDP).

Article 9. Security

- Data encrypted at rest and in transit.
- Access to case files limited to authorised people.
- Encrypted backups kept in the European Union.
- Human review of every action taken on a client's behalf.

Article 10. Tracking space and integrations

Where the engagement provides for it, the client's authorised teams access a secure tracking space or an application programming interface (API). Access is personal and limited to the users the client designates; connection logs are kept for the period stated below.

Article 11. Data breaches

If a breach is likely to create a risk to people's rights and freedoms, the office notifies the competent authority within the legal time limit (72 hours under the GDPR) and informs the people concerned where the risk is high, describing the measures taken.

Article 12. Retention periods

- Requests that do not lead to an engagement: 12 months after the last exchange.
- Engagement data: the length of the engagement, then 3 years.
- Evidence files and removal requests: 5 years, to defend rights.
- Verification documents: only as long as the verification, or the procedure that requires them, lasts.
- Accounting records: the applicable legal period.
- Technical logs: 12 months.

After these periods, data is deleted or irreversibly anonymised.

Article 13. Your rights

Under Law No. 09-08 you have the right of access, rectification and objection on legitimate grounds. If you are located in the European Union, you also have the rights to erasure, restriction and portability, and the right to withdraw your consent at any time.

To exercise these rights: privacy@bureauprotectiondigitale.fr. Proof of identity may be requested. A reply is given within the legal time limits.

Article 14. Complaints

- Morocco: 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
- Other European Union countries: the national data protection authority (list at edpb.europa.eu)

Article 15. Minors

Where a situation concerns a minor, the request is made by their legal representative.

Article 16. Changes

This policy may change. The version in force and its date are shown at the top of the document.