MarocAgency — Privacy, Consent & User Data Handling Policy

Version: 1.0

Effective Date: 2025-12-03

Approved by: Data Protection Officer / Compliance Manager

1. Purpose

Ensure that collection, processing, storage, and deletion of user or client personal data respects privacy, consent, and applicable data protection obligations — guaranteeing transparency, security, and user rights.

2. Scope

All user or client personal data handled by MarocAgency: contact information, leads data, analytics data, payment data (if applicable), cookies/usage data, and any PII collected via web projects, applications, marketing campaigns, or services.

3. Data Collection & Consent Principles

- Collect only data strictly required for the intended purpose (“data minimization”).
- Obtain explicit consent from users/clients before collecting or processing their personal data.
- Provide clear privacy notice explaining which data is collected, why, how it will be used, retention period, sharing practices, and user rights.

4. Data Storage & Protection

- Store personal data encrypted at rest and in transit.
- Restrict access to authorized personnel as defined by classification & access control policies.
- Maintain audit logs for data access and modifications.

5. Data Retention & Deletion / Right to Erasure & Portability

- Retain personal data only as long as needed, as defined in Data Retention Policy.
- On user/client request (or when purpose ends), support data deletion or anonymization / pseudonymization.
- Provide users with option to export their data (data portability).

6. Data Sharing & Third-Party Processors

- Sharing of personal data to third parties only with explicit user consent and under Data Sharing Policy.
- Third-party processors must sign DPA, comply with encryption and confidentiality standards, and follow retention/deletion rules.
- Log all data sharing events (what data, why, to whom, when).

7. Incident & Breach Handling for Personal Data

- In case of data breach involving personal data: follow Incident Response & Data Breach Policy.
- Notify affected data subjects and clients as required by legal or contractual obligations.

8. Data Subject Rights & Requests Handling

- Allow users/clients to request access, correction, deletion, or export of their personal data.
- Maintain process to handle such requests within defined timeframe (e.g. 30 days).
- Log requests and responses.

9. Compliance, Audits & Review

- Quarterly audits on personal data handling, consent logs, data access, data deletion requests.
- Annual review of privacy policy and data handling practices.
- Update when regulations change or company services evolve.

10. Roles & Responsibilities

- **Data Protection Officer / Compliance Manager:** ensure compliance, handle data requests, manage consent, coordinate audits.
- **Project / Data Owners:** collect minimal data, ensure consent is obtained, classify data correctly.
- **IT / DevOps & Security Team:** implement encryption, storage, access control, logging.
- **Employees / Developers / Contractors:** handle data responsibly, respect consent, follow policy guidance.