MarocAgency — Vendor & Third-Party Data Sharing Policy

Version: 1.0
Effective Date: 2025-12-03
Approved by: Compliance / Legal Manager

1. Purpose

Define strict rules and procedures for sharing or outsourcing any data or tasks to external vendors, subcontractors or third-party service providers — to preserve confidentiality, comply with data protection, and ensure contractual and legal safeguards.

2. Scope

Any sharing of data (client data, project data, backups, analytics, contact lists), or services outsourced to external parties (vendors, subcontractors, freelancers, third-party services, cloud providers) used by MarocAgency.

3. Prerequisites to Data Sharing**

- A valid Data Processing or Data Sharing Agreement (DPA) must be signed before sharing any sensitive or personal data.
- Vendor must demonstrate adequate security posture (encryption, access controls, data handling procedures).
- Data sharing must comply with classification policy: only data labelled “Public” or “Internal” may be shared freely; “Confidential” or “Highly Confidential” data requires explicit approval.

4. Data Transfer & Storage Rules

- All data transfers must be encrypted in transit (TLS, SFTP, VPN).
- Shared data must be handled and stored under the same security and retention requirements as internal data.
- Vendors must only store data as long as required; must follow MarocAgency’s Data Retention Policy.

5. Vendor Access Control & Audit

- Vendor access to systems/data must use designated accounts, with limited permissions per “least privilege”.
- All vendor activity should be logged and audited.
- Vendor must agree to periodic compliance audits by MarocAgency.

6. Data Return / Deletion After Contract End

- Upon contract completion or termination, vendor must return or securely delete all data obtained from MarocAgency.
- Deletion must be certified and logged.
- Data return (if required) must preserve encryption and integrity.

7. Exceptions & Emergency Sharing

- Any exception (urgent need, unexpected requirement) must be documented, justified, and approved by Compliance Manager.
- Temporary data sharing must follow minimal access, limited duration, and strict logging requirements.

8. Roles & Responsibilities

- **Compliance / Legal Manager:** approve contracts, monitor vendor agreements, enforce policy adherence.
- **Project / Data Owners:** evaluate data to share, classify sensitivity, request vendor sharing.
- **IT / Security Team:** configure secure data transfer, monitor vendor access, enforce encryption & access controls.
- **Vendors / Subcontractors:** comply with all policy conditions, sign DPA/NDA, maintain security, perform deletion or return data at contract end.

9. Policy Review & Update

- Review annually or when vendor relationships or regulatory requirements change.
- Maintain version history and documented approvals.