

Digital Personal Data Protection (DPDP) Policy

Anant Medicare & Legal Services Private Limited

(AM Legal Services / Anant Marketing & Associates)

Effective Date: August 2025

1. Purpose

Anant Medicare & Legal Services Private Limited ("Company", "we", "our", or "us") is committed to protecting the privacy and security of personal data entrusted to us by our clients, employees, vendors, business partners, and other stakeholders.

This Digital Personal Data Protection (DPDP) Policy has been established in accordance with the provisions of the Digital Personal Data Protection Act, 2023 (India) and applicable data protection regulations.

2. Scope

This Policy applies to:

- All employees, directors, consultants, and contractors of the Company.
 - All personal data collected, processed, stored, transmitted, or deleted by the Company.
 - All business operations, including:
 - Insurance Investigations
 - Background Verification (BGV)
 - Due Diligence Services
 - Medical & Legal Investigation Services
 - Employment Verification
 - Corporate Investigations
 - Vendor Verification
 - Claims Investigation Services
-

3. Definitions

Personal Data

Any data about an individual who is identifiable by or in relation to such data.

Data Principal

The individual to whom the personal data relates.

Data Fiduciary

An entity that determines the purpose and means of processing personal data.

Data Processor

Any person or organization processing personal data on behalf of the Company.

4. Data Collection

The Company may collect the following categories of personal data:

- Name
- Address
- Contact Number
- Email Address
- Date of Birth
- Government-issued Identification Documents
- Employment Information
- Educational Information
- Medical Information (where legally required)
- Insurance Claim Information
- Financial Information (where necessary)
- Photographs and Verification Records

Data is collected only for lawful and legitimate business purposes.

5. Purpose of Processing

Personal data may be processed for:

- Insurance claim investigations
- Background verification services
- Identity verification
- Employment screening
- Due diligence assignments
- Fraud detection and prevention
- Legal compliance requirements
- Client service delivery
- Contractual obligations

- Internal administration and operations
-

6. Consent Management

The Company processes personal data based on:

- Valid consent obtained from the Data Principal;
- Legitimate use permitted under applicable law; or
- Contractual and legal obligations.

Data Principals may withdraw consent where legally permissible.

7. Data Security Measures

The Company implements reasonable security safeguards including:

- Role-Based Access Control (RBAC)
 - Password-protected systems
 - Multi-factor authentication where applicable
 - Data encryption during transmission
 - Secure storage of records
 - Antivirus and endpoint protection
 - Access logging and monitoring
 - Employee confidentiality obligations
 - Periodic security reviews
-

8. Data Sharing and Disclosure

The Company may share personal data only with:

- Authorized clients
- Government authorities when legally required
- Courts, regulators, and law enforcement agencies
- Approved service providers and subcontractors
- Professional advisors and auditors

The Company does not sell personal data.

9. Data Retention

Personal data shall be retained only for as long as necessary to:

- Fulfill contractual obligations;
- Comply with legal requirements;
- Resolve disputes;
- Enforce legal rights; and
- Meet regulatory obligations.

Data no longer required shall be securely deleted or anonymized.

10. Rights of Data Principals

Subject to applicable law, Data Principals may:

- Access their personal data;
 - Request correction of inaccurate information;
 - Request deletion of personal data;
 - Withdraw consent;
 - Raise grievances regarding data processing;
 - Exercise rights available under the DPDP Act, 2023.
-

11. Grievance Redressal

Any concerns relating to personal data processing may be addressed to:

Grievance Officer

Anant Medicare & Legal Services Private Limited

Email: am.information@amlegalservices.org

Website: <https://amlegalservices.co.in/>

The Company will make reasonable efforts to resolve grievances within the timelines prescribed under applicable laws.

12. Employee Responsibilities

All employees and associates must:

- Protect confidential information.
- Access personal data only when authorized.

- Follow company security procedures.
- Report suspected data breaches immediately.
- Complete mandatory privacy and security awareness training.

Violation of this Policy may result in disciplinary action and legal consequences.

13. Data Breach Management

In the event of a personal data breach, the Company shall:

- Investigate the incident promptly;
 - Contain and mitigate the impact;
 - Notify affected parties and authorities where required by law;
 - Maintain records of incidents and corrective actions.
-

14. Third-Party Compliance

The Company requires vendors, contractors, and service providers handling personal data on its behalf to maintain appropriate security and privacy controls consistent with applicable legal requirements.

15. Policy Review

This Policy may be updated periodically to reflect changes in legal, regulatory, technological, or business requirements.

The latest version will always be available on the Company's website.

16. Contact Us

Anant Medicare & Legal Services Private Limited

Head Office: Ujjain, Madhya Pradesh, India

Email: am.information@amlegalservices.org

For any questions regarding this Policy, please contact us through the details provided above.

Last Updated: August 2025

Version: 1.0