



Digital Personal Data Protection (DPDP) Policy

Table of Contents

1. Purpose	2
2. Scope	2
3. Definitions	2
4. Types of Personal Data Collected	2
5. Purpose of Data Collection.....	3
6. Consent	3
7. Rights of Data Principals	4
8. Data Security Measures	4
9. Data Retention	4
10. Data Sharing	4
11. Data Breach Management	5
12. Data Processors & Third-Party Access	5
13. Employee Responsibility	5
14. Grievance Redressal.....	5
15. Approval.....	6

1. Purpose

This Digital Personal Data Protection Policy establishes the principles and procedures for the collection, processing, storage, use and protection of personal data by NDDB CALF Limited (NCL) in digital form.

The policy aims to ensure compliance with the provisions of the Digital Personal Data Protection Act, 2023 and to safeguard the privacy and personal data of employees, interns, clients, vendors and other stakeholders.

2. Scope

This policy applies to:

- All employees, interns, consultants, contractual staff and interns of the company
- All personal data processed by the laboratory in digital form
- Personal data collected through laboratory information systems, websites, emails, HR systems and electronic records.

This policy covers personal data relating to:

- Employees & Interns
- Clients and customer representatives
- Vendors and service providers
- Website users
- Visitors whose information is recorded digitally

3. Definitions

a) Personal Data

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

b) Data Principal

The individual to whom the personal data relates.

c) Data Fiduciary

The entity (NDDB CALF Ltd) that determines the purpose and means of processing personal data.

d) Processing

Includes collection, storage, use, sharing, analysis or deletion of personal data.

4. Types of Personal Data Collected

The NDDB CALF Limited may collect the following personal data:

Employee Data

- Name
- Contact details
- Identification documents
- Bank details for salary
- Educational and professional information

Client / Customer Data

- Name and designation
- Contact details (email, phone)
- Organization details along with GST, PAN, etc.
- Billing information

Vendor Data

- Contact information
- Organization details
- Bank details for payments
- Contract/AMC/ARC information

The NDDB CALF Limited does not intentionally collect sensitive personal data unless required for legitimate business or legal purposes.

5. Purpose of Data Collection

Personal data is collected only for legitimate purposes including:

- Employment and HR administration
- Customer communication and service delivery
- Sample submission and reporting of test results
- Billing and financial transactions
- Regulatory and ISO compliance
- Security and access control

6. Consent

Personal data will be processed only with the consent of the Data Principal, except where processing is permitted under law.

Consent must be:

- Free
- Specific
- Informed

- Unambiguous

Data Principals have the right to withdraw consent at any time.

7. Rights of Data Principals

Under the Digital Personal Data Protection Act, individuals have the right to:

- Access their personal data
- Request correction or updating of inaccurate data
- Request deletion of personal data when no longer necessary
- Withdraw consent for data processing
- File grievances regarding misuse of their personal data

Requests may be submitted to the Grievance Officer designated by the company.

8. Data Security Measures

The personal data shall be protected through reasonable security safeguards including but not limited to:

- Password-protected systems
- Role based access control
- Regular system updates and antivirus protection
- Secure storage of electronic records

Only authorized personnel shall have access to personal data.

9. Data Retention

Personal data shall be retained only for as long as necessary to fulfil the purpose for which it was collected or as required by applicable laws and regulatory requirements.

After the retention period, data will be securely deleted or anonymized.

10. Data Sharing

Personal data may be shared only when necessary with:

- Government authorities and regulators
- Statutory bodies, customers and stakeholders
- Banks and financial institutions
- Service providers assisting in business operations

Such sharing shall be limited to the minimum necessary information and shall comply with applicable legal requirements.

11. Data Breach Management

A personal data breach includes unauthorized data access, disclosure, alteration, loss or destruction of personal data.

In case of a suspected or actual breach:

- The incident shall be reported immediately to the Grievance Officer.
- Appropriate containment, mitigation and investigation measures shall be initiated.
- Notifications shall be made to relevant authorities and affected individuals if required under the Digital Personal Data Protection Act, 2023.

12. Data Processors & Third-Party Access

Third-party access to personal shall be strictly controlled.

All data processors must be bound by contractual DPDP obligations, including:

- Purpose limitation
- Confidentiality
- Access Controls
- Breach Notifications
- No unauthorized sub-processing

13. Employee Responsibility

All users must:

- Maintain confidentiality of personal information
- Use/Access personal data only for authorized purposes
- Follow company data protection policy/procedures
- Report any suspected data breach immediately

Violation may result in disciplinary action.

14. Grievance Redressal

Data principals may raise privacy or data protection grievances through the designated grievance redressal mechanism of the organization:

Grievance Officer: HR & Admin _ In-Charge

Department: Human Resource & Administration

The organization shall endeavour to resolve grievances within a reasonable time as specified in DPDP Act.

In the event a grievance is not resolved within prescribed timeframe, the Data Principal may approach Data Protection Board of India in accordance with applicable law.

15. Approval

This policy is approved by the competent authority and shall be effective from the date of issue.