Data Privacy and Protection Policy

Document No.	:ZLL/EDP/001
CREATED ON	16/06/2025
REVISION NO	: 00
EFFECTIVE DATE	:

1. Introduction

This Data Privacy and Protection Policy ("Policy") establishes guidelines for ZIM Laboratories Limited ("ZIM") to ensure the responsible collection, processing, storage, and sharing of personal data in compliance with applicable data protection laws and regulations, including the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. It applies to all employees, contractors, business partners, and third parties who handle personal data on behalf of the Company.

2. Purpose

The Policy aims at maintaining the privacy and protection of the confidential information including personal information of Suppliers, Customers, Consumers and business partners (“you”, “your”, “individual”, “stakeholder”) of the Company and simultaneously complying with all the laws and regulations.

The Company has framed this policy to:

- provide protection of the privacy of all stakeholders related to their personal data,
- specify the flow and usage of personal data, create a relationship of trust between individuals and entities processing the personal data,
- protect the rights of Individuals whose personal data are processed and retained by the Company, and
- create a framework for organisational and technical measures in processing and storage of data

This policy is outlines for best practices regarding the collection, use, processing, disclosure, and security of personal and sensitive personal data, with a particular focus on the stringent privacy requirements necessary in the pharmaceutical industry.

3. Scope and Applicability

This policy is applicable to all the employees, contractors, vendors, interns, associates, customers and business partners including all such third party/ies who may receive personal information, have access to personal information collected or processed, or who provide information to the organization, regardless of geographic location. The Company expects its employees, contractors, vendors, interns, associates, customers and business partners

including third party's to support and abide by this policy and principles with respect to the data that they collect and / or handle, or are involved in the process of maintaining or disposing. This policy aims at protecting the data of the stakeholders. No third party may access personal information held by the organization without having first entered into a confidentiality agreement. Policy covers all forms of personal data, including but not limited to:

- Customer information
- Employee data
- Clinical trial participant information
- Vendor and partner details

4. Definitions

- **Personal Information**: As per the IT Rules, any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.
- **Personal Data:** Any Information that relates to an identified or identifiable individual, including name, address, contact details, and other similar identifiers described below:-

❖ **Basic Identity Information**:

- Name
- Address
- Phone number
- Email address

❖ **Identifiers:**

- National Identification Number (like Social Security Number, Aadhaar)
- Passport number
- driver's license number

❖ **Financial Data**:

- Credit card details
- Bank account information
- Transaction history

❖ **Sensitive Personal Data Information (SPDI)**

- Health records
- Genetic or biometric data
- Racial or ethnic origin

- Political opinions
- Sexual orientation
- Religious or philosophical beliefs

❖ **Online Data**:

- Cookies
- Device IDs
- Geolocation data
- Social media activity

- **Consent**: - Refers to the explicit, informed, and voluntary permission given by an individual for the collection, processing, and sharing of their personal or sensitive data. Consent must be obtained after fully informing the individual about the purpose and intended use of the data, ensuring transparency and legality in data handling practices. Additionally, Consent obtained at the time of employment initiation shall remain valid for the duration of the individual's employment unless revoked in writing.
- **Data subject: -** refers to the individual whose personal or sensitive personal data is being collected, processed, stored, or shared by an organization. The **data subject** is the person to whom the data relates and who has rights over their personal information.

5. Collection of Personal Information

The organisation may collect personal information, including SPDI, through various means:

- **Directly from you**: When Data subject provide information through organisation's website, applications, or customer interactions.
- **Automatically**: Using cookies, web beacons, and other tracking technologies.
- **From third parties**: Such as partners, affiliates, or service providers.

6. Purpose of Collection and Use of Personal Information

The Company uses the personal data of the Individuals only for valid legal purpose. The said data is used only upon consent of the Individuals. The personal data collected is necessary to fulfil a contract, protect vital interests of the Individuals or those of other persons, or to comply with law. This enables the Company to provide relevant and related products or services. It is not compulsory to provide personal data, but in some cases, the non-provision of certain personal data will cause the inability to provide information relating to best deals for related products or services. The data is processed for legitimate interests, taking into consideration interests, rights, and expectations of the Individuals. The organisation may collect and use personal information, including SPDI, for the following purposes:

- **Provision of Services**: To provide the services or products requested by data subject
- Execution of agreements with Customers, Suppliers and Business Partners;
- Research and development and data analysis;
- **Verification**: For identity verification and authentication purposes.
- **Communication**: To communicate with Data subject regarding services, updates, or customer support.
- **Regulatory Compliance**: To comply with legal obligations under applicable laws and regulations including reporting obligations to regulatory authorities, and also while hiring the candidate background check .
- Processing payments
- **Internal Operations**: To improve services, hire and train employees, manage relationships with customers, vendors, and other stakeholders.

7. Disclosure of Personal Information

The organisation does not disclose the personal information to third parties without the prior written consent of the data subject except under the following circumstances:

- **With consent**: Personal information may be shared with third parties if the data subject has provided explicit consent. Consent obtained at the time of employment initiation shall remain valid for the duration of the individual's employment unless revoked in writing.
- **Legal compliance**: The organisation may disclose personal data when required by law or legal process. The policy effectively aligns with the Information Technology Act 2000 and the IT Rules 2011, ensuring legal compliance.
- **Service providers**: The organisation may share information with third-party service providers who assist in providing services, subject to confidentiality agreements.

However, the data that is already available in the public domain or known to the third party prior to such disclosure, then the Company shall not be under any obligation to protect such data.

8. Security Practices and Procedures

The Organisation implement reasonable security practices and procedures as required under the IT Rules to protect personal information, including SPDI, to ensure the protection of personal and sensitive personal data of the data subject. These measures include:

- **Access Controls**: Restricting access to personal information to authorized personnel only on a need-to-know basis.
- **Regular Audits**: Conducting regular security audits to ensure compliance with applicable laws and standards.

9. Data Storage and Retention of Personal Information

The data is stored in electronic as well as physical form. The personal data is collected only to the extent that is necessary for the purposes of processing of such personal data All personal data collected under this Policy shall be retained only for as long as necessary to fulfil the purpose for which it was collected, or as may be required under applicable laws and internal policies. Upon the expiry of the retention period, the data shall be securely deleted, anonymized, or archived in accordance with the Company's data disposal procedures.

Only **authorized personnel** shall be permitted to collect, access, process, or store personal data. Authorized personnel shall include designated members of the **IT Department, Data Protection Officer (if appointed), and other relevant departments** as determined by internal access control protocols. The assignment of authorization shall be role-based and strictly on a need-to-know basis.

The Company shall implement and regularly review internal controls, including access logs, audit trails, and system permissions, to ensure that personal data is handled in compliance with applicable data protection laws and to prevent unauthorized access, alteration, or misuse.

Any breach of access control protocols or misuse of data by authorized personnel will result in disciplinary and/or legal action as per Company policy and applicable law.

10. Data Security

The data collected and stored online is secured with passwords, pins, antivirus, etc. to protect from any viruses/spam/malware attack. Whereas the data collected and stored offline is secured by keeping it in a safe place/room with appropriate security i.e. CCTV surveillance, maintaining register/record of the person accessing/visiting the data room. The Company takes necessary measures to prevent the data from any kind of fraud and to comply with all applicable laws at all times. Staff shall be provided access to Personal Data only to the extent necessary to serve the applicable Business Purpose and to perform their job. Staff who access Personal Data shall meet their confidentiality obligations.

11. Individual Rights

Under the IT Rules, individual's data subject has the following rights concerning individual personal and sensitive information:

- **Access and Review**: Individuals can request access and review to their personal data and inquire about how it is processed.
- **Correction**: The right to request correction of inaccurate or incomplete data.
- **Grievance Redressal**: The right to file a complaint with designated Grievance Officer if an individual believes that their personal data has been misused or mishandled.

12. DATA BREACH MANAGEMENT and Grievance Officer

- Any data breach shall be reported immediately to the Data Protection Officer (DPO) or relevant authorities, as required by law.
- The ZIM shall take prompt action to mitigate risks and notify affected individuals where necessary.
- The breach response process shall align with the IT Act's cybersecurity and data protection provisions.

In compliance with Rule 5(9) of the IT Rules 2011 and Rule 17 of IT Rules 2017, the ZIM have appointed a Grievance Officer to act as the point of contact to address any concerns or complaints regarding the handling of personal information.

Grievance Redressal Mechanism

In accordance with the scope of this Policy, all grievances or concerns related to the processing, handling, or security of personal data shall be addressed in a timely and structured manner. The **Grievance Officer** for this Policy shall be the **Head of Information Technology (IT Head)**, who shall serve as the primary point of contact for all data protection-related complaints.

Upon receipt of a grievance, the Grievance Officer shall acknowledge the complaint within **3 (three) working days** and initiate a review. Depending on the nature and complexity of the grievance, the IT Head may redirect the matter to the appropriate internal department or function (e.g., Legal, HR, Compliance, etc.) for further investigation and resolution.

All grievances shall be addressed and resolved within **30 (thirty) days** from the date of receipt. In cases requiring more time, the complainant shall be informed of the expected timeline and reason for the delay.

For any concerns, complaints, or requests regarding personal data or privacy matters, individuals may write to:

Grievance Officer
Vikrant Ambhore
Deputy Manager-EDP
grievanceit@zimlab.in

Grievance Officer:
Email :- grievanceit@zimlab.in
Address :- A: B-21/22, MIDC Area, Kalmeshwar, PIN: 441 501, Nagpur, MS, India

According to **Rule 5(9)** of the Act, the Grievance Officer must **acknowledge** and **act on a complaint** regarding the handling of personal or sensitive personal data **within one month (30 days)** from the date of receiving the complaint.

13. LEGAL COMPLIANCE

The ZIM shall comply with all applicable provisions of the IT Act, including Section 43A **(Compensation for failure to protect data)** and Section 72A **(punishment for disclosure of information in breach of a lawful contract)**.

The ZIM shall ensure that any cross-border data transfer aligns with the IT Act and relevant international data protection frameworks.

14. International Transfers of Data

If the personal data may be transferred to and stored on servers located outside country of residence of the Data subject. The organisation shall ensure that appropriate safeguards are in place to protect Personal data of the data subject, in compliance with applicable laws and regulations.

a) Cross-Border Transfers:

While transferring data internationally, the organisation shall comply with the necessary legal requirements, including data protection agreements and contractual clauses.

15. Changes to This Policy

The organisation shall reserve the right to modify or update this policy from time to time in compliance with legal and regulatory changes. Any updates will be posted on website or communicated through other appropriate means.

16. Contact Details

For any inquiries or concerns regarding this Policy, data subjects may contact:
Data Protection Officer (DPO)
Name: ZIM Laboratories Limited:

Email :- grievanceit@zimlab.in
Address :- A: B-21/22, MIDC Area, Kalmeshwar, PIN: 441 501, Nagpur, MS, India

This Privacy Policy is in compliance with the Information Technology Act, 2000 and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.