

Horizon Tech Solutions Data Protection Policy

Policy Effective Date: October 26, 2025

1. Introduction & Scope

This policy outlines the principles and procedures for the collection, processing, and protection of personal data at Horizon Tech Solutions. It applies to all employees, contractors, and third-party vendors who handle personal data on our behalf, in compliance with the Digital Personal Data Protection Act, 2023.

2. Key Principles

At Horizon Tech Solutions, we adhere to the following data protection principles:

- **Lawfulness and Transparency:** We will process personal data fairly, lawfully, and in a transparent manner.
- **Purpose Limitation:** Data will be collected for specified, explicit, and legitimate purposes only and will not be further processed in a manner that is incompatible with those purposes.
- **Data Minimization:** We will collect and process only the personal data that is strictly necessary for the purpose for which it is collected.
- **Accuracy:** We will take all reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date.
- **Storage Limitation:** We will not retain personal data for longer than is necessary to fulfill the purpose for which it was collected.
- **Integrity and Confidentiality:** We will ensure data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

3. Roles and Responsibilities

- **Data Fiduciary:** Horizon Tech Solutions is the Data Fiduciary. The ultimate responsibility for compliance with this policy and the DPDP Act rests with the company's leadership.
- **Data Protection Officer (DPO):** Mr. Amit Sharma has been appointed as the DPO. He is responsible for overseeing compliance, advising on data protection matters, and acting as the primary point of contact for the Data Protection Board of India and Data Principals. He can be reached at dpo@horizontech.in.

- **All Employees:** Every employee is responsible for adhering to this policy and for promptly reporting any suspected data breaches or security incidents to the DPO.

4. Consent and Lawful Basis

- **Consent:** We will obtain valid consent from Data Principals using a clear affirmative action (e.g., a checkbox on a web form). Our consent forms and privacy notices will be provided in clear and plain language.
- **Withdrawal of Consent:** A Data Principal can withdraw their consent at any time, and we will make it as easy to withdraw consent as it was to give it.

5. Data Principal Rights

We are committed to upholding the rights of Data Principals under the DPDP Act. We have established internal procedures to handle requests for:

- **Right of Access:** Data Principals can request confirmation of whether their data is being processed and, if so, to access that data.
- **Right to Correction & Erasure:** Data Principals can request the correction, completion, or erasure of their personal data.
- **Grievance Redressal:** All grievances will be handled by the DPO and will be addressed within a period of 30 days.

6. Data Security

- **Technical Measures:** We will use appropriate technical measures such as end-to-end encryption for sensitive data, multi-factor authentication for internal systems, and regular vulnerability assessments.
- **Organizational Measures:** We will limit data access on a "need-to-know" basis, implement regular employee training on data protection, and conduct periodic internal audits.

7. Data Breach Management

In the event of a data breach, we will follow our established Data Breach Response Plan. This plan includes:

- **Detection and Containment:** Swiftly identifying the breach and taking immediate steps to contain it.
- **Assessment:** Assessing the nature, extent, and potential consequences of the breach.
- **Notification:** Notifying the Data Protection Board of India and affected Data Principals within 72 hours of becoming aware of the breach, where required by the Act.

8. Third-Party Data Processing

We will only engage third-party vendors who can demonstrate their commitment to data protection. All third-party agreements will include a Data Processing Agreement (DPA) with clauses that ensure compliance with the DPDP Act.

9. Cross-Border Data Transfers

All cross-border data transfers will be carried out in strict compliance with the DPDP Act. Personal data will only be transferred to a jurisdiction that is not restricted by the Indian government and with appropriate safeguards in place.

Policy Review: This policy will be reviewed annually or whenever there is a significant change in the law or company's data processing activities.