23 Finverse Digital Personal Data Protection (DPDP) Compliance Policy

Effective Date: [Insert Date]
Last Updated: [Insert Date]

1. Purpose

23 Finverse ("Company", "we", "our", or "us") is committed to protecting the privacy and security of personal data entrusted to us by our customers, employees, Channel Partners (CPs), Distributor Partners (DPs), vendors, service providers, and other stakeholders.

This Digital Personal Data Protection (DPDP) Compliance Policy ("Policy") establishes the principles and controls governing the collection, processing, storage, sharing, retention, and protection of personal data in accordance with the **Digital Personal Data Protection Act, 2023 (DPDP Act)** and other applicable laws.

This Policy applies to all employees, directors, consultants, contractors, interns, partners, and third parties processing personal data on behalf of 23 Finverse.

---

2. Scope

This Policy applies to all personal data processed by 23 Finverse through:

- The 23 Finverse web application.
- Mobile applications (where applicable).
- Customer support channels.
- Sales and marketing activities.
- Human resources processes.
- Vendor and partner management.
- Digital communication platforms.
- Cloud infrastructure and internal business systems.

It covers personal data in electronic and, where applicable, physical form.

---

3. Consent Management

23 Finverse shall process personal data only where there is a lawful basis under the DPDP Act, including valid consent where required.

Consent shall be:

- Free, specific, informed, and unambiguous.
- Obtained before processing where legally required.
- Recorded and maintained in an auditable manner.
- Capable of being withdrawn as easily as it was given.

Individuals shall be informed about:

- The categories of personal data collected.
- The purpose of processing.
- The consequences of refusing or withdrawing consent, where applicable.
- Available privacy rights and grievance mechanisms.

Withdrawal of consent shall not affect processing already completed or processing permitted under applicable law.

---

4. Data Collection

23 Finverse collects only the personal data reasonably necessary to provide its services and fulfil legitimate business, contractual, or legal obligations.

Personal data may include:

- Identity information.
- Contact details.
- Account credentials.
- Financial and payment information.
- KYC documentation where applicable.
- Communication records.
- Device and technical information.
- Transaction history.
- Usage analytics.

Data collection shall be:

- Fair and transparent.
- Limited to stated purposes.
- Accurate and up to date, where reasonably practicable.
- Relevant and proportionate to the intended purpose.

Personal data shall not be collected through unlawful or deceptive means.

---

5. Data Sharing

Personal data may be shared only where necessary and lawful, including with:

- Payment service providers.
- Banking and financial institution partners.
- Cloud infrastructure providers.
- Identity verification and KYC service providers.
- Technology vendors.
- Analytics and communication service providers.
- Professional advisers.
- Government authorities or regulators where required by law.

Before sharing personal data, 23 Finverse shall:

- Assess the necessity of the disclosure.
- Ensure appropriate contractual safeguards are in place.
- Limit the data shared to what is reasonably necessary.
- Require recipients to maintain appropriate security and confidentiality standards.

23 Finverse does not sell personal data to third parties.

---

6. Data Storage

Personal data shall be stored using secure systems designed to protect confidentiality, integrity, and availability.

Security measures may include:

- Encryption of data in transit and at rest.
- Secure cloud infrastructure.
- Firewalls and network security controls.
- Endpoint protection.
- Secure backup procedures.
- Continuous system monitoring.
- Physical security controls for infrastructure where applicable.

Access to stored personal data shall be restricted to authorized personnel with a legitimate business need.

---

7. Data Breach Management

23 Finverse maintains procedures for detecting, investigating, managing, and responding to actual or suspected personal data breaches.

Where a breach occurs, the Company shall:

- Contain the incident promptly.
- Assess the nature and scope of the breach.
- Evaluate potential risks to affected individuals.
- Notify competent authorities where required by applicable law.
- Inform affected individuals where legally required or appropriate.
- Implement corrective and preventive measures.
- Maintain records of all significant data breach incidents.

All employees and representatives must immediately report any suspected personal data breach to the designated Information Security or Compliance team.

---

8. Access Controls

Access to personal data shall be governed by the principles of **least privilege** and **need-to-know**.

23 Finverse shall implement appropriate access control measures, including:

- Unique user accounts.
- Strong authentication mechanisms.
- Multi-factor authentication for privileged access, where applicable.
- Role-based access controls.
- Periodic access reviews.
- Timely removal of access upon termination or role changes.
- Monitoring of privileged user activity.

Unauthorized access to personal data is strictly prohibited.

---

9. Data Retention

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

- Fulfil the purposes for which it was collected.
- Comply with legal and regulatory obligations.
- Resolve disputes.
- Prevent fraud.
- Enforce contractual rights.
- Meet audit and accounting requirements.

Retention periods shall be documented and periodically reviewed.

Once retention requirements expire, personal data shall be securely deleted, anonymized, or irreversibly destroyed.

---

10. Data Deletion

Individuals may request deletion of their personal data, subject to applicable legal and contractual obligations.

Upon receiving a valid request, 23 Finverse shall:

- Verify the identity of the requester.
- Assess whether deletion is legally permissible.
- Delete or anonymize eligible personal data within a reasonable timeframe.
- Retain only such information as is required by law or for legitimate business purposes.

Deletion requests may be declined where retention is necessary to comply with statutory obligations, resolve disputes, prevent fraud, or establish, exercise, or defend legal claims.

---

11. Audit Logs

23 Finverse shall maintain appropriate audit logs relating to the processing of personal data to support security, accountability, and regulatory compliance.

Audit logs may include records of:

- User authentication.

- Access to personal data.
- Data modifications.
- Data exports.
- Administrative actions.
- Security events.
- System changes.

Audit logs shall be:

- Protected against unauthorized modification or deletion.
- Retained for an appropriate period based on legal, regulatory, and operational requirements.
- Reviewed periodically for unusual or unauthorized activity.

---

12. Third-Party Processors

Where third parties process personal data on behalf of 23 Finverse, the Company shall exercise appropriate due diligence before engagement.

Third-party processors shall be required to:

- Process personal data only in accordance with documented instructions.
- Implement reasonable technical and organizational security measures.
- Maintain confidentiality.
- Notify the Company promptly of any personal data breach.
- Permit compliance reviews or audits where contractually agreed.
- Delete or return personal data upon termination of services, unless retention is required by law.

23 Finverse remains responsible for ensuring that third-party processors comply with applicable contractual and legal obligations.

---

13. Employee Responsibilities

All employees and authorized representatives shall:

- Protect personal data from unauthorized disclosure.
- Follow Company privacy and security policies.
- Complete mandatory privacy and information security training.
- Report suspected privacy incidents immediately.

- Use personal data only for authorized business purposes.
- Maintain confidentiality even after the end of employment or engagement.

Failure to comply with this Policy may result in disciplinary action.

---

14. Policy Governance and Review

This Policy shall be reviewed periodically to ensure continued compliance with applicable laws, regulatory guidance, technological developments, and business requirements.

23 Finverse reserves the right to amend this Policy at any time. Updated versions shall become effective upon publication or internal communication.

---

15. Contact Information

For questions regarding this Policy, privacy practices, or the processing of personal data, please contact:

23 Finverse

Data Protection & Compliance Team: privacy@23finverse.com

Compliance Team: compliance@23finverse.com

Support: support@23finverse.com

Registered Office: 5th Floor Esplanade One Mall Rasulgarh Bhubaneswar ODisha 751010