W.S. INDUSTRIES (INDIA) LIMITED

POLICY ON USAGE OF PERSONAL DATA AND COMPLIANCE WITH THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

---

1. PREAMBLE

This Policy is framed in accordance with the provisions of the **Digital Personal Data Protection Act, 2023** ("DPDP Act") and other applicable laws, to establish a structured framework for the collection, processing, storage, access, retention and protection of personal data by W.S. Industries (India) Limited ("the Company").

The Company, being a listed entity, recognises the importance of protecting personal data of employees, directors, shareholders, customers, vendors and other stakeholders, and is committed to ensuring compliance, accountability and transparency in data processing activities.

---

2. OBJECTIVE

This Policy aims to:

- Ensure lawful, fair and transparent processing of personal data
- Establish purpose limitation and data minimisation principles
- Implement reasonable security safeguards
- Define access control mechanisms
- Provide a governance and compliance framework

---

3. SCOPE

This Policy applies to:

- All personal data processed in digital form by the Company
- Any personal data processed through Company systems, software or third-party platforms

This Policy applies to all directors, officers, employees, consultants and authorised personnel of the Company.

---

4. DEFINITIONS

- **Personal Data**: Any data about an identifiable individual processed in digital form.
- **Data Fiduciary**: The Company, which determines the purpose and means of processing personal data.
- **Processing**: Collection, storage, use, sharing, modification, or deletion of personal data.

---

5. PRINCIPLES OF DATA PROCESSING

The Company shall adhere to the following principles:

5.1 Lawful Purpose

Personal data shall be processed only for lawful and legitimate purposes including employment administration, statutory compliance, contractual obligations, regulatory filings, and business operations.

5.2 Purpose Limitation

Data shall be used strictly for the purpose for which it is collected.

5.3 Data Minimisation

Only such personal data as is necessary for the intended purpose shall be collected and processed.

5.4 Accuracy

Reasonable steps shall be taken to ensure that personal data is accurate and updated when required.

5.5 Storage Limitation

Personal data shall not be retained beyond the period required under applicable laws or business necessity.

---

6. EMPLOYEE DATA & PAYROLL INFORMATION

6.1 Employee KYC data (including PAN, Aadhaar, bank account details, address, etc.) shall be collected solely for employment, payroll, taxation and statutory compliance purposes.

6.2 Access to such data shall be governed by the **need-to-know principle**.

6.3 The payroll software/system shall, wherever technically feasible:

- Display personal identifiers in masked form by default
- Allow full visibility only to authorised personnel
- Restrict full access to instances where modification, statutory filing, audit, or verification is required
- Maintain audit trails of access and modification

6.4 Unrestricted routine visibility of full KYC data shall be avoided unless operationally justified.

---

7. ACCESS CONTROL AND SECURITY SAFEGUARDS

The Company shall implement reasonable technical and organisational safeguards including:

- Role-based access control
- Password-protected systems
- Data encryption (where feasible)
- Access logs and periodic review
- Secure storage and backup protocols
- Confidentiality undertakings from authorised personnel

---

8. DATA SHARING

Personal data may be shared only:

- With statutory authorities where required by law
- With banks, consultants, auditors and service providers strictly for legitimate purposes
- Under contractual confidentiality obligations

No personal data shall be shared for unrelated purposes.

---

9. RETENTION AND DELETION

Personal data shall be retained:

- As required under tax, labour and corporate laws

- For legitimate business purposes

Upon expiry of retention period, data shall be deleted or anonymised in a secure manner.

---

10. DATA BREACH MANAGEMENT

Any suspected or actual personal data breach shall be:

- Immediately reported to the Executive Directors / Chief Financial Officer / Audit Committee / Designated Officer, from time to time.
- Assessed for impact
- Reported to regulatory authorities and affected individuals where required under law

---

11. RIGHTS OF INDIVIDUALS

The Company shall provide mechanisms for individuals to:

- Seek information regarding processing
- Request correction or updating of data
- Raise grievances

A Grievance Officer shall be designated for handling such requests.

The Company may adopt a dual-level grievance redressal structure:

Primary Grievance Officer:
Mr. Vinoth – Executive HR & Admin
Email: hradmin@wsigroup.in
Contact: +91 95137 02766

If one is not satisfied with the resolution provided, such person may escalate the matter to:

Appellate / Escalation Authority:
Chief Financial Officer / Whole-Time Director
Email: cfo@wsigroup.in

---

12. GOVERNANCE AND RESPONSIBILITY

- The Board shall have overall oversight of data governance.

- The HR Head and IT Head shall ensure implementation of operational safeguards.
- All employees handling personal data shall adhere strictly to this Policy.
- The report on such compliance, shall be placed before board on periodic basis.

---

13. REVIEW OF POLICY

This Policy shall be reviewed periodically or upon any amendment to applicable laws, whichever is earlier.

****

This policy is approved by the Board of Directors at their meeting held on 14.05.2026