DPDPA_PG_P_PIMS_CH_GGEPIL

Policy Name: Privacy Governance Policy and Privacy Information Management Systems (PIMS) Charter

Version: 1.0

Owner: Data Protection Officer (DPO)

Approved by: Executive Sponsor

Effective Date: 02.03.2026

Applies to: All employees, contractors, contractor's contractors, suppliers, customers, service providers and any other third parties of GGEPIL

1. Purpose

GGEPIL establishes a Privacy Information Management System (PIMS) aligned to ISO/IEC 27701 to ensure lawful, fair, and transparent processing of personal data in compliance with India's Digital Personal Data Protection (DPDP) Act, 2023.

2. Scope

This policy covers all personal data processing activities for employees, customers, suppliers, visitors, candidates, and any individuals whose personal data is processed by GGEPIL, across physical sites and/or offices in Palsana - Surat, Panoli, Chittaurgarh, Faridabad, Karad, Ranipet, Telangana, Mota Randha and Alang, and digital systems (on-premises and cloud).

3. Governance Structure

- Executive Sponsor: Provides resources and strategic oversight.

- Data Protection Officer (DPO): Accountable for privacy compliance and engagement with the Data Protection Board (DPB).

- Privacy Steering Committee: Cross-functional representatives (IT/Data Security, Legal/Compliance, HR/Admin, Operations, Sales/Marketing, Procurement, Technical Services, PR & CSR, Projects, Accounts/Finance/Taxation, Company Secretary).

- Personal Identifiable Information (PII) Roles:

  - PII Controller: GGEPIL determines the purposes and means for most of the internal data

- PII Processor: GGEPIL may act as processor for client projects where purposes are determined by clients.

4.Data Protection Officer

The Data Protection Officer (DPO) is appointed by GGEPIL, which is a Significant Data Fiduciary, or is a Data Fiduciary who may be considered as a Significant Data Fiduciary by our Central Government. The DPO must be based in India.

The DPO reports directly to the Board of Directors of GGEPIL, thereby ensuring independence and accountability.

The role of Data Protection Officer includes:

4.1.Serving as a single point of contact for

- Data principals (data subjects) for grievances and queries
- The Data Protection Board of India during audits and investigations.

4.2.Monitoring organizational compliance with DPDP Act and Rules, including:

- Notice and consent frameworks
- Data retention, deletion, and minimization practices
- Handling of data subject rights (access, correction, erasure)
- Cross-border data transfer adherence

4.3.Overseeing Data Protection Impact Assessments (DPIAs) for high-risk processing

activities and advising on mitigation strategies

4.4.Managing grievance redressal, ensuring timely response to data principals and

escalation to the Board of Directors, if unresolved

4.5.Acting as the liaison with regulators, cooperating with the Data Protection Board in compliance reporting, audits, and investigations

4.6.Developing and conducting training and awareness programs to embed data protection culture across the organization

4.7.Auditing and monitoring data practices, including conducting internal reviews and recommending corrective action for non-compliance

4.8.Advises on and implements security measures and privacy-by-design standards, collaborating with CIO, CISO and CDO to safeguard personal data.

5. Policy Principles

5.1.Privacy by Design: Every process and policy in GGEPIL should, to the extent possible, include Data Privacy and Information Security as key elements, so that the requirements of DPDP Act are taken care of by during thee organizational design phase/stage itself.

5.2.Lawfulness: Every processing activity must have a valid legal basis (consent, contract, legal obligation, legitimate uses, vital interests).

5.3.Purpose Limitation & Minimization: Collect only what is necessary for defined purposes; avoid secondary use without a fresh basis.

5.4.Transparency: Provide clear, plain-language privacy notices prior to processing.

5.5.Data Subject Rights: Enable access, correction, erasure, withdrawal of consent, grievance redressal, and nomination.

5.6.Security Safeguards: Implement appropriate technical and organizational measures (TOMs).

5.7.Accountability: Maintain records, logs, audits, and continuous improvement of the PIMS.

6. Broad Roles and Responsibilities

6.1.DPO: Maintain policies, conduct training, oversee audits, manage breaches and DP Board interactions.

6.2.IT/Security: Implement controls (encryption, access, logging, SIEM), automate retention/deletion.

6.3.Legal/Compliance: Update contracts/Data Protection Agreements (DPAs), manage lawful basis, cross-border transfers, and regulatory monitoring.

6.4.HR/Operations: Ensure HR data handling and site processes comply.

6.5.Procurement/Projects: Enforce vendor privacy due diligence and Data Protection Assessments and DPAs.

7. Oversight & Review

- Quarterly Steering Committee review of Key Performance Indicators (right Service Level Agreement, consent logs, deletion success, vendor risk).

- Annual management review; policy refreshes; internal audits.

8. Exceptions

Exceptions require documented risk assessment, approval by DPO and Executive Sponsor, and compensating controls.

9. Enforcement

Non-compliance may lead to disciplinary action as per HR policy and regulatory reporting duties under DPDP Act.