PRIVACY AND PERSONAL DATA PROTECTION POLICY

Enterprise Policy for Personal Data Governance

Entity	Fortuna Engineering Private Limited
Document Reference	FEPL/PRIVACY & PERSONAL DATA PROTECTION POLICY/00/15.07.2026
Version	0.0 (First Approved Policy)
Effective Date	15.07.2026
Policy Owner	Head – Human Resources & Compliance
Approval Authority	Board of Directors / Corporate Management Team
Classification	Internal Corporate Policy

This Policy establishes Fortuna Engineering Private Limited's enterprise-wide framework for lawful, fair, transparent and secure handling of Personal Data. It is supported by function-specific notices, retention schedules, information-security procedures and contractual controls.

Document Control

Version	Date	Prepared / Reviewed by	Approved by	Nature of change
0.0	15.07.2026	HR, IT, Legal / Compliance	Executive Director	First comprehensive privacy and personal data protection policy

Benchmarking Basis and Drafting Approach

This redraft is designed primarily for compliance with Indian law and operational use within a manufacturing enterprise, while incorporating globally recognised privacy governance concepts. The Policy should be read as an internal governance document; separate privacy notices may be required for employees, applicants, visitors, vendors, customers and website users.

Benchmark	How reflected in this Policy
India – Digital Personal Data Protection framework	Lawful processing, notice, consent and specified legitimate uses; data-principal rights; security safeguards; breach response; grievance redressal; processors; retention and erasure; nomination and children's data.
EU General Data Protection Regulation (where applicable)	Transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality, accountability, privacy by design/default, processor contracts, impact assessments and broader individual rights.
ISO/IEC 27701:2025	Privacy Information Management System principles, controller/processor accountability, documented controls, continual improvement and integration with information-security governance.
NIST Privacy Framework	Risk-based privacy governance organised around identifying, governing, controlling, communicating and protecting data-processing activities.
ISO/IEC 27001:2022	Information-security management controls supporting confidentiality, integrity, availability, risk treatment, incident response and continual improvement.

Contents

1. Purpose
2. Scope and Applicability
3. Definitions
4. Privacy Principles
5. Governance, Accountability and Roles
6. Personal Data Inventory and Classification
7. Lawful Grounds and Processing Conditions
8. Privacy Notices and Consent Management
9. Purposes and Categories of Processing
10. Data Quality, Minimisation and Access Control
11. Individual Rights and Grievance Redressal
12. Children and Persons Requiring Lawful Guardianship
13. Sharing, Processors and Third Parties
14. Cross-Border Transfers
15. Information Security and Privacy by Design
16. CCTV, Access Control, Biometrics and Monitoring
17. Retention, Archival and Secure Disposal
18. Personal Data Breach and Incident Management
19. Data Protection Impact Assessments and Change Management
20. Records, Training, Audit and Assurance
21. Workforce Responsibilities and Disciplinary Consequences
22. Exceptions, Review and Amendment
23. Contact and Escalation

Annexure A – Minimum Retention Framework

Annexure B – Data Subject Request Workflow

Annexure C – Personal Data Breach Response Matrix

Annexure D – Implementation Actions Before Approval

1. Purpose

Fortuna Engineering Private Limited ("Fortuna" or the "Company") is committed to handling Personal Data lawfully, fairly, transparently and securely. This Policy establishes the minimum governance, operational and technical requirements for collecting, using, storing, sharing, transferring, retaining and deleting Personal Data in the course of the Company's business.

The Policy is intended to protect individuals, support contractual and statutory compliance, preserve customer and workforce trust, and ensure that privacy risk is integrated into business and technology decisions.

2. Scope and Applicability

This Policy applies to all Personal Data processed by or on behalf of Fortuna in digital form and, where such data is digitised or forms part of an organised filing system, in physical form. It applies across all plants, offices, warehouses, project sites, systems and functions controlled by the Company.

- All directors, employees, fixed-term personnel, trainees, apprentices, interns and contract labour where Fortuna determines or controls the processing;
- Job applicants, former employees, dependants, nominees and emergency contacts;
- Customer, supplier, logistics, consultant, auditor, visitor and other business-contact data;
- All third parties processing Personal Data for or on behalf of Fortuna, including payroll, HRMS, cloud, security, recruitment, insurance, banking, travel and IT service providers;
- Personal Data received from group entities, customers or partners under contract.

This Policy does not by itself create a legal basis to process data. Each processing activity must have an identified purpose, a lawful ground, an appropriate notice and the controls required by applicable law and contract.

Confidential business information, technical drawings, PPAP records, PFMEA, control plans, pricing, manufacturing know-how and other proprietary information are governed by the Company's confidentiality and information-security requirements. They fall within this Policy only to the extent they contain Personal Data.

3. Definitions

Term	Meaning for this Policy
Applicable Data Protection Law	The Digital Personal Data Protection Act, 2023 and rules/notifications brought into force thereunder, the Information Technology Act, 2000 and applicable rules, and any foreign data protection law that applies to a specific processing activity.
Personal Data	Any data about an individual who is identifiable by or in relation to such data.
Digital Personal Data	Personal Data in digital form, including data collected in non-digital form and subsequently digitised.
Data Principal / Individual	The individual to whom Personal Data relates. Where applicable, this includes a parent or lawful guardian acting for a child or person requiring lawful guardianship.
Data Fiduciary / Controller	The person or entity that determines the purpose and means of processing Personal Data. Fortuna will ordinarily act as Data Fiduciary for its own workforce, visitor and business-contact data.
Data Processor / Processor	A person or entity that processes Personal Data on behalf of a Data Fiduciary or Controller.
Processing	Any operation performed on Personal Data, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, sharing, transmission, restriction, erasure or destruction.
Consent	A free, specific, informed, unconditional and unambiguous indication of the individual's wishes by clear affirmative action, capable of being withdrawn as easily as it is given.
Personal Data Breach	Any unauthorised processing, accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, or compromise of confidentiality, integrity or availability of Personal Data.
Sensitive / High-Risk Personal Data	Personal Data requiring enhanced protection because misuse may create material harm, including government identifiers, financial data, health/disability data, biometrics, precise location, disciplinary records and authentication credentials.

4. Privacy Principles

- Lawfulness, fairness and transparency: process Personal Data only on a valid basis and communicate material processing clearly.
- Purpose limitation: collect and use Personal Data only for specified, explicit and legitimate purposes; incompatible secondary use requires fresh assessment and, where required, fresh notice or consent.
- Data minimisation: collect only data that is adequate, relevant and reasonably necessary.
- Accuracy: keep Personal Data complete and up to date where accuracy is relevant to the purpose.
- Storage limitation: retain identifiable data only for as long as required for the documented purpose, law, contract or defence of claims.
- Security and confidentiality: apply safeguards proportionate to sensitivity, volume, context and risk.
- Accountability: maintain evidence of decisions, controls, notices, consents, contracts, requests, incidents, training and audits.
- Privacy by design and default: embed privacy requirements into systems, forms, projects, processes and vendor selection from the outset.

5. Governance, Accountability and Roles

5.1 Corporate Management Team / Board

- Approve this Policy and material privacy risk positions;
- Ensure adequate resources and oversight;
- Review significant incidents, high-risk processing and material non-compliance.

5.2 Privacy Officer / Data Protection Compliance Officer

The Company shall designate a suitably senior officer as Privacy Officer. Until separately designated in writing, the Head – Human Resources & Compliance will coordinate privacy governance with IT, Legal/Secretarial, Finance, Security and relevant business functions.

- Maintain the Personal Data Register and processing inventory;
- Coordinate notices, rights requests, grievances, breach assessment and regulator/data-principal communications;
- Review processor contracts, high-risk projects and retention schedules;
- Report material privacy risks and implementation status to management at least annually.

5.3 Department Heads and Process Owners

- Identify Personal Data used in their processes and ensure a lawful purpose, minimum collection, appropriate access and approved retention;
- Ensure staff and vendors follow this Policy;
- Escalate new systems, monitoring, analytics, AI, biometrics, cross-border transfers or material changes before deployment.

5.4 IT and Information Security

- Implement technical safeguards, logging, access management, vulnerability management, backups and incident response;
- Maintain system inventories and support secure deletion, restoration and forensic preservation;
- Assess security posture of processors and service providers.

6. Personal Data Inventory and Classification

Each function shall identify and document what Personal Data it processes, from whom it is collected, purpose, lawful ground, system/location, access, recipients, processor, transfer location, retention period and deletion method. The inventory shall be reviewed at least annually and when a material process changes.

Classification	Examples	Minimum treatment
Restricted / High Risk	Aadhaar/PAN and other government identifiers; bank details; payroll; health/disability; biometrics; background-verification reports; disciplinary/investigation records; passwords, tokens and authentication data.	Strict need-to-know access, encryption or equivalent protection, enhanced logging, approved transfer channels and shorter retention where feasible.
Confidential Personal Data	Addresses, phone numbers, photographs, employment records, performance records, attendance, CCTV, visitor logs and personal correspondence.	Role-based access, secure storage/transmission and documented retention.
Business Contact Data	Name, title, company, business email/phone and business correspondence.	Use for legitimate business communications, with access and retention proportionate to purpose.

7. Lawful Grounds and Processing Conditions

Before processing begins, the process owner shall identify and document the lawful ground. Depending on the law applicable to the activity, this may include consent, performance of a contract, compliance with law, specified legitimate uses, protection of vital interests, employment-related purposes permitted by law, or legitimate interests where recognised and appropriately balanced.

- Consent shall not be used merely as a formality where processing is mandatory by law or necessary to administer employment or a contract.
- Where consent is relied upon, refusal or withdrawal shall not result in unrelated adverse consequences, although the Company may be unable to provide the specific optional service dependent on that data.
- Personal Data obtained from another person or organisation shall be verified as having been lawfully collected and shareable for the intended purpose.
- High-risk or unusual processing requires Privacy Officer review before commencement.

8. Privacy Notices and Consent Management

Fortuna shall provide clear privacy information at or before collection, or as soon as reasonably practicable where data is received indirectly. Notices shall be concise, understandable and available in a language reasonably accessible to the relevant individuals.

- Identity and contact details of Fortuna and the relevant grievance/privacy contact;
- Categories of Personal Data and source;
- Purposes and lawful ground;
- Whether provision is mandatory or voluntary and consequences of non-provision;
- Recipients, processors and material cross-border transfers;
- Retention criteria;
- Rights and the method to exercise them;
- How to withdraw consent where consent is relied upon;
- Material automated decision-making or monitoring, if any.

Consent records shall capture the notice/version shown, date/time, method, purpose and withdrawal status. Bundled, pre-ticked or unclear consent must not be used for optional processing.

9. Purposes and Categories of Processing

Activity	Typical Personal Data	Purposes
Recruitment and onboarding	Identity/contact data, CV, education/employment history, interview notes, references, background checks, offer and joining records.	Evaluate suitability, communicate, verify credentials, meet legal/contractual requirements and establish employment.
Workforce administration	Employee and dependant details, attendance, leave, shifts, performance, training, discipline, travel, benefits and emergency contacts.	Manage employment, workforce planning, safety, welfare, performance and legal obligations.
Payroll, tax and statutory benefits	PAN, Aadhaar where lawfully required, bank details, salary, tax, PF/ESIC and insurance data.	Pay remuneration, administer benefits, remit statutory deductions and maintain records.
Occupational health and safety	Medical fitness, incident/injury, disability accommodation and emergency information.	Protect health and safety, fulfil factory/labour obligations and provide reasonable support.
Customers and suppliers	Business contact details, correspondence, authority, contracts, purchase orders, invoices, quality and audit records.	Contracting, supply-chain execution, quality assurance, payment, audit and relationship management.
Physical security and access	Visitor identity, organisation, vehicle, access-card data, entry/exit, CCTV and incident records.	Safety, access control, asset protection, investigation and legal compliance.

Activity	Typical Personal Data	Purposes
IT and communications	User IDs, device identifiers, login/activity logs, email and collaboration metadata, cybersecurity alerts and support records.	Provide systems, secure networks, detect threats, investigate misuse and maintain business continuity.
Legal, audit and governance	Litigation, claims, investigations, whistleblowing, compliance reviews and regulatory submissions.	Establish, exercise or defend legal rights; comply with law, customer requirements and audits.

10. Data Quality, Minimisation and Access Control

- Forms and systems shall avoid collecting fields that are not demonstrably required.
- Copies of government identifiers shall not be collected or retained unless required or clearly justified. Aadhaar handling shall follow applicable UIDAI requirements, including masking and secure verification practices where relevant.
- Personal Data shall not be stored in personal email, unapproved cloud storage, removable media or local devices except where authorised and protected.
- Access shall be based on job role, least privilege and segregation of duties; privileged access shall be reviewed periodically.
- Access shall be promptly modified or revoked upon transfer, role change, suspension or separation.
- Personal Data sent externally shall use approved channels and be limited to the minimum necessary.

11. Individual Rights and Grievance Redressal

Subject to applicable law, identity verification, legal privilege, confidentiality of others and permitted exemptions, individuals may request:

- Information about and access to Personal Data being processed;
- Correction, completion or updating of inaccurate or incomplete data;
- Erasure of data that is no longer necessary or lawfully required;
- Withdrawal of consent for future processing where consent is the basis;
- Grievance redressal concerning processing or exercise of rights;
- Nomination of another individual to exercise rights in the event of death or incapacity, where provided by law;
- Additional rights available under a foreign law applicable to the particular processing, which may include restriction, objection, portability and protection against certain solely automated decisions.

Requests shall be submitted to the contact in Section 23. The Company will acknowledge, verify identity, assess scope, search relevant systems, consult affected functions and respond within the period prescribed by applicable law or, where no period is prescribed, without unreasonable delay. No fee will ordinarily be charged unless permitted by law for manifestly unfounded or excessive requests.

A requester shall first use Fortuna's grievance mechanism before approaching an external authority where applicable law so requires. The Company shall not retaliate against an individual for making a good-faith privacy request or complaint.

12. Children and Persons Requiring Lawful Guardianship

Fortuna does not ordinarily offer consumer services to children. Where Personal Data of a child or a person requiring lawful guardianship is processed—for example, dependant records, apprentices, benefits, emergency or statutory records—the process owner shall confirm the applicable age threshold and obtain verifiable consent or authority from the parent/lawful guardian where required.

- Such data shall not be used for tracking, behavioural monitoring or targeted advertising.
- Collection shall be limited to the employment, benefit, safety, statutory or welfare purpose.
- Access shall be strictly limited and retention reviewed when the purpose ends.

13. Sharing, Processors and Third Parties

Fortuna does not sell or rent Personal Data. Personal Data may be shared only where necessary and authorised, including with government bodies, regulators, courts, law-enforcement agencies, banks, insurers, auditors, professional advisers, customers, group entities and approved service providers.

Before appointing a processor, the responsible function shall conduct proportionate due diligence and ensure a written contract that addresses:

- Documented instructions, purpose, duration and categories of data;
- Confidentiality and personnel controls;
- Appropriate security safeguards;
- Sub-processor approval and flow-down obligations;
- Assistance with rights requests, incidents, audits and regulatory obligations;
- Breach notification to Fortuna without undue delay and with sufficient detail;
- Return or secure deletion at end of service;
- Audit, assurance and evidence rights;
- Cross-border transfer restrictions and location transparency;
- Business continuity and exit support.

Processor access shall be periodically reviewed. High-risk processors shall be subject to enhanced diligence, contractual review and security assurance.

14. Cross-Border Transfers

Personal Data may be transferred outside India only after confirming that the transfer is permitted under applicable Indian restrictions and any customer or sector-specific obligations. Where foreign privacy law applies, the Company shall implement an appropriate transfer mechanism and supplementary safeguards as required.

- The Personal Data Register shall identify the destination country and recipient;
- Transfers shall be limited to the stated purpose and minimum data;
- Contracts shall require equivalent confidentiality, security, incident and deletion controls;
- The Privacy Officer and IT shall review material new cross-border transfers before commencement.

15. Information Security and Privacy by Design

Fortuna shall maintain reasonable security safeguards proportionate to the nature, volume and risk of Personal Data. These safeguards form part of the Company's broader information-security management system.

- Multi-factor authentication for appropriate systems and remote/privileged access;
- Role-based access, strong authentication, periodic access review and segregation of duties;
- Encryption or equivalent controls for high-risk data in transit and at rest where appropriate;
- Secure configuration, patching, endpoint protection, firewalls, logging and monitoring;
- Backups, restoration testing, business continuity and disaster recovery;
- Secure software and change-management practices;
- Physical security, clean-desk/clean-screen controls and secure records storage;
- DLP or equivalent controls for sensitive engineering/customer data where proportionate;
- Periodic vulnerability assessment and penetration testing based on risk;
- Privacy and security review before acquiring or materially changing systems.

Default system settings shall limit visibility, collection, retention and sharing to what is necessary. Test and training environments should use masked or synthetic data wherever practicable.

16. CCTV, Access Control, Biometrics and Monitoring

CCTV and access-control systems may be used for safety, security, incident prevention, access management, investigation and protection of people and assets. Monitoring shall be necessary, proportionate and communicated through notices or signage.

- Cameras shall not be placed in areas where individuals reasonably expect a high degree of privacy.
- Live or recorded access shall be limited to authorised Security, IT, HR, Legal/Compliance or management personnel with a legitimate need.
- Footage shall not be used for routine performance surveillance unless lawfully justified, notified and approved.
- Audio recording and facial recognition shall not be enabled without specific legal and privacy assessment.
- Biometric attendance or access systems require documented necessity, enhanced security, restricted access and a defined retention/deletion process.
- Requests for footage disclosure shall be documented and limited to the relevant period and purpose.

17. Retention, Archival and Secure Disposal

Personal Data shall be retained according to an approved retention schedule based on law, contract, customer requirements, operational necessity and limitation periods. "Keep indefinitely" is not an acceptable default unless specifically justified.

- At the end of retention, data shall be securely erased, anonymised or destroyed so that it cannot reasonably be reconstructed.
- Deletion shall cover active systems, shared drives and local records. Backups may be deleted through normal rotation where immediate deletion is technically impracticable, provided they remain protected and are not restored for ordinary use.
- Legal hold, investigation, audit or dispute requirements may suspend deletion for identified records.
- Paper records shall be cross-cut shredded or destroyed by an approved vendor with appropriate custody controls.
- Disposal of devices and media shall follow secure wiping or physical destruction standards.

18. Personal Data Breach and Incident Management

Any actual or suspected loss, unauthorised access, disclosure, alteration, unavailability, malware event, misdirected communication, lost device, credential compromise or improper disposal involving Personal Data must be reported immediately through the Company's incident channels.

- Immediate contacts: Department Head, Privacy Officer / Head – HR & Compliance, and Lead IT Administrator / Management Representative.
- Employees and contractors must preserve evidence and must not conceal, delete or independently communicate about the incident.
- IT and the incident team shall contain the event, preserve evidence, determine affected data and individuals, assess harm, document decisions and implement remediation.
- The Privacy Officer shall determine whether and when notification to the Data Protection Board/other regulator, affected individuals, customers, insurers or law enforcement is required.
- Processor contracts shall require immediate notice to Fortuna, even where all facts are not yet known.
- Lessons learned and corrective actions shall be tracked to closure.

19. Data Protection Impact Assessments and Change Management

A documented privacy impact assessment shall be completed before high-risk processing begins or materially changes. Triggers include:

- Large-scale processing of workforce or visitor data;
- Biometrics, facial recognition, health data or systematic monitoring;
- AI or automated decision tools affecting recruitment, performance, discipline, access or benefits;
- New employee-monitoring technologies;
- Combining datasets in a way that materially increases identifiability or impact;
- New cross-border hosting or high-risk processor;
- Processing likely to create significant harm, exclusion, discrimination or loss of control for individuals.

The assessment shall record necessity, proportionality, legal basis, notice, data flows, risks, controls, residual risk and approval. High residual risk requires management decision and, where required, consultation with an appropriate authority or adviser.

20. Records, Training, Audit and Assurance

- Maintain processing records, notices, consent records, vendor assessments, processor contracts, rights-request logs, incident records, impact assessments and retention evidence.
- Provide induction and periodic privacy/security training to relevant personnel, with enhanced training for HR, IT, Security, Finance, Procurement and management.
- Conduct periodic audits and control reviews based on risk and customer requirements.
- Track corrective and preventive actions to closure.
- Review privacy metrics at least annually, including requests, incidents, overdue deletions, processor reviews, training completion and high-risk projects.

21. Workforce Responsibilities and Disciplinary Consequences

- Access Personal Data only for authorised work purposes and only to the extent required.
- Do not share credentials, bypass controls, photograph records/screens, or copy data to personal devices or accounts.
- Verify recipients before sending data and use approved secure channels.
- Follow clean-desk, clear-screen, secure printing and confidential disposal requirements.
- Immediately report suspected incidents, phishing, lost devices, excessive access or policy violations.
- Cooperate with investigations, requests, audits and remediation.

Breach of this Policy may result in access restriction, disciplinary action up to and including termination, recovery of loss, contractual remedies and legal action, subject to applicable law, service rules and principles of natural justice.

22. Exceptions, Review and Amendment

Any exception must be documented, time-bound, risk-assessed and approved by the Privacy Officer, IT/Information Security and the relevant authority based on the level of risk. Exceptions shall include compensating controls and an expiry/review date.

This Policy shall be reviewed at least annually and earlier upon material legal change, regulator guidance, customer requirement, major incident, system transformation or business restructuring. The Company may amend the Policy, but material changes shall be communicated to affected personnel and reflected in relevant notices and procedures.

23. Contact and Escalation

For privacy questions, individual rights requests, grievances or incident reporting, contact:

Function	Human Resources & Compliance Department / Privacy Officer
Company	Fortuna Engineering Private Limited
Address	E-108/E-109, MIDC Ambad, Nashik – 422010, Maharashtra, India
Email	Girish.shinde@fortunaengineering.com
Internal escalation	Head – HR & Compliance; Lead IT Administrator / Management Representative; Corporate Management Team

Annexure A – Minimum Retention Framework

The periods below are policy defaults and must be validated against applicable labour, tax, corporate, factory, social-security, customer, insurance, litigation and contractual requirements. Where requirements conflict, the longer lawful period may be applied with documented rationale.

Record category	Baseline retention approach
Unsuccessful applicant records	12–24 months after closure of recruitment, unless a longer period is consented to or required for a claim.
Employee personnel file	Employment period plus 7 years, subject to specific statutory records requiring longer retention.
Payroll, tax, PF, ESIC and statutory benefit records	At least 8 years or the longer period required by applicable law/audit.
Attendance, leave, shift and wage-supporting records	As prescribed by applicable labour/factory law; policy default 7 years unless a different period applies.
Medical/occupational health and safety records	Period required by law and nature of exposure/claim; segregated with restricted access.
Background-verification reports	As long as necessary for the recruitment/employment decision and claims; avoid indefinite retention of source documents.
Visitor and access logs	90 days to 1 year based on site-security need, unless linked to an incident or customer requirement.
CCTV footage	Normally 30–90 days, unless preserved for an incident, legal hold or investigation.
Supplier/customer business contacts and contracts	Business relationship plus 8 years or applicable limitation/tax/contract period.
IT access and security logs	90 days to 1 year, or longer for critical systems/security investigations based on risk.
Rights requests and privacy grievances	At least 3 years after closure, or longer if required for regulatory/claim defence.
Personal Data breach records	At least 7 years after closure, or longer where litigation/regulatory action is possible.
Consent records	Duration of processing plus period necessary to demonstrate lawful consent and manage withdrawal.

Annexure B – Data Subject Request Workflow

1. Receive and log the request through the designated channel.
2. Acknowledge receipt and provide a reference number.
3. Verify identity proportionately; do not collect excessive identity proof.
4. Clarify scope where necessary and identify applicable law/deadline.
5. Search relevant systems and consult process owners, Legal and IT.
6. Assess exemptions, third-party confidentiality, privilege and legal holds.
7. Correct, provide, erase, restrict or otherwise act as legally required.
8. Respond in clear language, explain any refusal and available escalation.
9. Document completion and retain the request file under the retention schedule.

Annexure C – Personal Data Breach Response Matrix

Timing	Owner	Minimum action
0–1 hour	Reporter / Department / IT	Escalate, contain immediate exposure, preserve evidence, disable compromised access where safe.
Same working day	Incident team	Identify systems, data types, approximate individuals, cause, ongoing risk, processor/customer involvement.
Without undue delay	Privacy Officer / Legal / Management	Assess legal and contractual notification obligations and prepare communications.
As required by applicable law	Authorised notifier	Notify regulator/board and affected individuals with known facts, mitigation and contact route.
Post-containment	Process owner / IT / HR / Legal	Root cause, remediation, recovery, monitoring, disciplinary/vendor action and lessons learned.

Annexure D – Implementation Actions Before Approval

Action	Suggested owner	Reason
Appoint and name the Privacy Officer / grievance contact	Management / HR	Mandatory operational owner and public contact.
Create a dedicated privacy email address	IT / HR	Replace placeholder in Section 23 and all notices.
Prepare separate privacy notices	HR / Legal / Compliance	At minimum: employees, applicants, visitors/CCTV, vendors/business contacts and website.
Build the Personal Data Register	All functions coordinated by Privacy Officer	Record data flows, lawful grounds, recipients, systems, transfers, retention and deletion.
Approve a detailed retention schedule	HR / Finance / Legal / IT / Quality	Validate Annexure A against law, customer and IATF requirements.
Update processor/vendor contracts	Procurement / Legal / IT	Add privacy, security, incident, deletion, sub-processing and audit clauses.
Establish rights-request SOP and register	Privacy Officer / HR / IT	Define identity verification, search, response and escalation.
Establish breach-response SOP and notification templates	IT / Privacy Officer / Legal	Align with DPDP Rules, contracts and cyber-incident obligations.
Review Aadhaar, biometrics, CCTV and employee monitoring	HR / Security / IT / Legal	Confirm necessity, notices, security, retention and lawful basis.
Conduct role-based training	HR / IT	Induction plus annual refreshers; enhanced modules for high-risk functions.
Approve periodic privacy audit metrics	Management	Quarterly implementation tracking and annual management review.

Approval

	Prepared / Reviewed by	Approved by
Name	Girish K Shinde	Eashwar Suriyanarayanan
Designation	Sr. Manager - HR	Executive Director
Signature		
Date	15.07.2026	15.07.2026