

Digital Personal Data Protection Policy

DPDP Act 2023 and DPDP Rules 2025

1.0 Identity purpose and scope

1.1 Sun Tech Precision is a partnership firm with GSTIN 29ADKFS1829A1Z3, located at #685, 5 & 6, Tigalarapalya Main Road, Near New Indian National High School, Peenya 2nd Stage, Bengaluru, Karnataka - 560058, India. Our website is <https://suntechprecision.com>. This policy is effective from 09 October 2026 and establishes responsibilities for lawful handling of digital personal data across our website and business operations. It applies to partners, employees, contractors and service providers processing data under STP's authority.

1.2 The scope includes personal data collected digitally and information collected in non-digital form that is subsequently digitized. It covers website enquiries, WhatsApp communications, customers, suppliers, recruitment, employment, payroll, attendance, CCTV, premises visitors and other authorized activities. Paper records that are not digitized remain subject to applicable confidentiality, security and other legal duties even where outside the DPDP Act's scope.

2.0 Legal framework and phased commencement

2.1 STP shall comply with the Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 in accordance with their notified commencement and applicability. The commencement notifications provide an immediate institutional phase, a one-year phase for specified Consent Manager provisions, and an eighteen-month phase for the principal processing duties, individual rights and related rules, calculated from publication of the relevant Gazette notifications. STP shall track amendments and any change to that schedule.

2.2 This policy establishes organizational requirements from its effective date. A statutory duty or remedy not yet commenced shall not be represented as already enforceable solely because it is described here. During transition, applicable Information Technology Act, 2000 obligations, the SPDI Rules, 2011 and other binding requirements shall continue to be observed until lawfully amended, repealed or displaced. Where rules overlap, STP shall satisfy each applicable requirement.

3.0 Roles and accountability

3.1 STP is a Data Fiduciary where it determines the purpose and means of processing personal data. A service provider acting on STP's instructions is a Data Processor for that activity. Where STP processes information solely on a customer's instructions, the respective roles and obligations shall be documented. Different activities within the same relationship may have different roles.

3.2 The Managing Partner is accountable for privacy governance, allocation of resources, approval of significant processing changes and grievance oversight. Department heads shall identify data held in their processes and implement the relevant controls. IT and service providers shall implement technical controls under assigned responsibilities. Appointment of a processor does not remove STP's statutory accountability.

3.3 STP shall not describe its grievance contact as a statutory Data Protection Officer merely by designation. If notified as a Significant Data Fiduciary, STP shall appoint the required India-based Data Protection Officer, arrange independent audit and impact assessments, and implement the additional statutory measures applicable to that status.

4.0 Data inventory and purpose assessment

4.1 Each process owner shall maintain a register identifying data categories, affected individuals, source, purpose, legal basis, systems, recipients, processors, transfers, retention period and responsible owner. New forms, software, vendors, surveillance systems and material changes shall undergo privacy review before introduction.

4.2 The review shall establish necessity, proportionality and the minimum information needed; identify less intrusive alternatives; assess unauthorized-access and misuse risks; and specify controls. Information shall not be collected because it might be useful later. Publicly available information shall not be assumed exempt without checking the legal conditions under which it was made public.

5.0 Notices and transparent collection

5.1 A clear, independently understandable notice shall be provided at or before consent-based collection. It shall identify STP, itemize the personal data sought, explain each specified purpose and the relevant service or use, and provide practical means for withdrawal, rights requests and grievances. Where required, the notice shall also explain how to approach the Data Protection Board.

5.2 Notices shall be available in English or an applicable Eighth Schedule language as required by law and supported by an accessible request process. The notice shown and version accepted shall be recorded. General acceptance of website terms shall not be used as a substitute for specific consent where consent is required.

5.3 For data previously collected on consent before the operative statutory commencement, the required transition notice shall be issued as soon as reasonably practicable in accordance with the Act. Existing databases shall be assessed for source, purpose, consent evidence, continued necessity and lawful retention; old possession alone does not authorize new use.

6.0 Consent and permitted uses

6.1 Consent shall be free, specific, informed, unconditional and unambiguous, indicated by clear affirmative action, and limited to data necessary for the specified purpose. Pre-selected boxes, silence, vague bundled permissions and a supplier's blanket consent on behalf of all employees shall not be relied upon. Optional promotional, testimonial or publicity use shall be distinguished from necessary operational use.

6.2 Where STP relies on a permitted use under section 7, the precise statutory condition shall be assessed and documented. This may include qualifying voluntarily supplied information for a specified purpose, employment-related purposes, or an applicable emergency or legal function. Contract performance or general legitimate interest shall not be treated as a free-standing catch-all basis under the DPDP Act.

6.3 Consent records shall identify the individual or relevant reference, purpose, notice version, date, method and subsequent changes. Once registered Consent Manager mechanisms are legally operative and relevant, STP shall support valid consent choices communicated through applicable arrangements; it shall not treat an unverified intermediary as a registered Consent Manager.

7.0 Withdrawal and consequences

7.1 Individuals may withdraw consent through sales@suntechprecision.com or an equally accessible channel appropriate to the original interaction. Process owners shall identify affected activities and processors, stop consent-based processing within a reasonable time and notify the individual of any necessary service consequences. Withdrawal shall not attract a punitive charge.

7.2 Lawful processing completed before withdrawal remains unaffected. Information that must continue to be processed or retained under law shall be separated from optional uses, restricted and retained only for the justified period. Withdrawal shall be recorded to prevent accidental reactivation of a discontinued purpose.

8.0 Website enquiries and communications

8.1 The website collects contact enquiries and offers optional WhatsApp chat. STP shall use information submitted through these channels to respond and manage the requested interaction. It shall not automatically enroll an enquirer into recurring promotions or use contact details for an unrelated purpose. Enquiry forms shall avoid requesting sensitive records or unnecessary information about third parties.

8.2 WhatsApp and similar external services operate under their own terms and privacy practices. STP shall offer email as an alternative, minimize sensitive exchanges and assess business use of external platforms. Introducing analytics, advertising trackers, online payment, account or application functions requires a new privacy review and the necessary notices and choices before deployment.

9.0 Employees applicants and contractors

9.1 HR and relevant administrators shall limit collection to lawful recruitment, employment administration, payroll, benefits, safety, statutory compliance and protection of legitimate employer interests within the applicable legal framework. Employment status does not authorize unlimited monitoring or unrestricted use of personal information. Access to financial, health and identity records shall be restricted by role.

9.2 Unsuccessful applications shall be retained only for a justified recruitment period or another disclosed lawful purpose. Reference checks and background verification shall be proportionate, conducted through appropriate authorization and communicated to the individual where required. Records of dependants or emergency contacts shall be limited to the relevant benefit or emergency purpose.

9.3 Employees shall be told how their information is used and how to raise concerns without retaliation. Personal information shall not be uploaded to unapproved AI services, private cloud accounts or unauthorized messaging groups. Access and devices shall be reviewed on role changes and termination, with records preserved only for legitimate ongoing needs.

10.0 CCTV biometric attendance and premises visitors

10.1 CCTV, where operated, shall use clear site notices and be limited to justified security locations. Access to footage shall be controlled and logged, and disclosure shall require authorization or a valid legal basis. Continuous audio recording, facial recognition or other expanded surveillance shall not be introduced without a separate necessity and legal assessment.

10.2 Routine CCTV footage shall normally be overwritten within 30 days unless a documented incident, investigation, legal obligation or applicable mandatory retention requirement requires preservation. Preserved footage shall be restricted to the relevant event and reviewed until the reason for retention ends. Applicable statutory retention requirements override the routine overwrite cycle for records to which they apply.

10.3 Biometric attendance, where used, shall be subject to a specific notice, appropriate lawful basis and security controls over templates and devices. Raw biometric images shall not be retained merely for convenience. Process owners shall assess alternatives, vendor access, storage locations and deletion on cessation of the attendance purpose, subject to lawful retention. Aadhaar-based processing shall not be introduced without separately confirming its legal permissibility.

10.4 Visitor records shall be limited to information reasonably needed for identification, safety, access and incident response. Routine copying of full identity documents shall be avoided where a less intrusive verification is sufficient. Visitor registers shall not be left publicly visible or used as an unsolicited marketing list.

11.0 Children and lawful guardians

11.1 A child means an individual below eighteen years for the purposes of the Act. Before processing a child's personal data where consent is required, STP shall obtain verifiable parental or lawful guardian consent and exercise due diligence concerning the adult's identity and authority. Any exemption shall be relied on only within its notified scope and conditions.

11.2 STP shall not undertake prohibited tracking, behavioral monitoring or targeted advertising directed at children, or processing likely to cause a detrimental effect on their well-being. Limited processing for employee benefits, lawful apprenticeships or site safety shall be separately assessed rather than treated as a blanket exception.

11.3 Where a person with a disability has a lawful guardian and the relevant consent provisions apply, STP shall verify the guardian's appointment and authority. Supported communication and accessible request handling shall be provided as reasonably required; a disability alone does not establish guardianship or remove the individual's rights.

12.0 Accuracy access control and security

12.1 Before using data to make a decision affecting an individual or disclosing it to another Data Fiduciary, the process owner shall take appropriate steps to ensure completeness, accuracy and consistency. Corrections shall be propagated to relevant systems and recipients where necessary. Unverified information shall be identified as such and shall not be knowingly represented as confirmed fact.

12.2 Security controls shall include role-based access, strong authentication where appropriate, encryption or suitable masking, secure transmission, patching, malware protection, physical safeguards and controlled backups. Logs and monitoring shall support detection of unauthorized activity. Recovery arrangements shall protect confidentiality, integrity and availability, and restoration shall be tested proportionately to operational risk.

12.3 When applicable DPDP security provisions commence, the minimum safeguards and required one-year preservation of relevant logs and data shall be implemented. Where CERT-In directions apply, STP shall maintain the required ICT logs securely for at least 180 days within Indian jurisdiction, synchronize system clocks appropriately and maintain the required incident point of contact. A longer applicable legal period shall prevail for the relevant records.

13.0 Processors and sub-processors

13.1 A processor shall be appointed only after proportionate assessment of its capability, access, security and hosting arrangements. Written terms shall state the authorized purpose, categories of information, confidentiality, safeguards, approved sub-processors, international access, incident notification, rights assistance, audit evidence, retention and return or deletion obligations.

13.2 Processors shall not repurpose information or engage an unapproved sub-processor contrary to the agreement. STP shall maintain relevant oversight and shall require prompt correction of identified gaps. The contract shall require immediate incident escalation, with an initial report within four hours of awareness where STP information may be affected, so that statutory deadlines can be met; a processor shall not wait for a complete forensic report.

14.0 Sharing and international transfers

14.1 Disclosures shall be limited to necessary recipients and supported by a lawful basis. Customer or certification audits shall receive only the information needed for the verification, with unnecessary employee or visitor identifiers removed where possible. Regulatory demands shall be validated and fulfilled through authorized channels, preserving evidence of the scope and legal basis.

14.2 International transfers and remote overseas access shall be assessed against operative government restrictions, sectoral requirements, contractual confidentiality and export controls. Processor contracts and technical controls shall reflect the decision. Any Significant Data Fiduciary localization requirement shall be followed if applicable; STP shall not assume that every overseas transfer is either automatically prohibited or automatically permitted.

15.0 Retention legal holds and disposal

15.1 Process owners shall maintain purpose-based retention schedules and review information when its purpose ends or consent is withdrawn. Retention mandated by law shall be distinguished from commercial convenience. Quality-record or contract periods shall not be applied indiscriminately to unrelated personal information.

15.2 When operative, the minimum one-year retention required by rule 8(3) for covered personal data, associated traffic information and processing logs shall be applied for its specified purposes, followed by deletion unless a further legal requirement justifies retention. Any schedule-specific inactivity rule and advance erasure notification shall be applied only if STP and the activity fall within the prescribed class; no universal three-year inactivity rule is assumed for a CNC business.

15.3 Legal holds shall identify the records and reason, restrict use and be reviewed periodically. Disposal shall include authorized processor copies and controlled backup handling, with a record of completion. Irreversibly anonymized information may be retained where re-identification is not reasonably possible; merely replacing a name with a code does not necessarily anonymize data.

16.0 Personal data breach response

16.1 Any suspected loss, unauthorized disclosure, alteration, destruction or loss of access affecting personal data shall be reported internally without delay. The response team shall contain the incident, preserve evidence, assess the affected individuals and data, document decisions and coordinate recovery. The absence of confirmed financial harm does not automatically mean that a reportable personal-data breach has not occurred.

16.2 When the applicable DPDP breach rules are operative, STP shall notify each affected individual and the Board without delay in the prescribed manner. Individual communications shall explain the nature and timing, likely consequences, mitigation, practical protective steps and contact. The Board shall receive the initial available particulars promptly and the required detailed update within 72 hours of awareness, or a longer period expressly allowed by it; the update period does not postpone the initial notice.

16.3 Independent CERT-In duties shall be assessed immediately. Where its directions apply to a listed cyber incident, reporting shall occur within six hours of noticing or being informed of the incident. Customer and other regulatory deadlines shall also be met. Media clearance or incomplete investigation shall not delay mandatory reporting. Root causes and effectiveness of corrective actions shall be reviewed after containment.

17.0 Individual rights and verification

17.1 STP shall provide a practical channel for requests concerning access to processing information, correction, completion, updating, erasure, withdrawal, grievance redressal and nomination as applicable under law. Access responses shall cover the information required by the Act, including an appropriate summary and relevant recipient information, subject to lawful limitations. No broader statutory right to portability is implied by this policy.

17.2 Identity shall be verified proportionately using the existing relationship, registered contact or another suitable method. Information requested solely for verification shall be minimized and protected. A request register shall record receipt, verification, responsible owner, decision and response. Refusal or partial fulfillment shall include a reason and available escalation route where lawful.

17.3 A nomination request shall identify the nominee and necessary verification particulars, without unnecessary collection. A nominee's authority to exercise rights upon death or incapacity shall be verified before disclosure. Nomination for privacy rights does not itself determine inheritance or ownership of commercial assets.

18.0 Grievances contact and statutory escalation

18.1 Requests shall be addressed to the Managing Partner, Sun Tech Precision, at sales@suntechprecision.com, or by post to #685, 5 & 6, Tigalarapalya Main Road, Near New Indian National High School, Peenya 2nd Stage, Bengaluru, Karnataka - 560058, India. Privacy requests should use the subject "Privacy Request"; complaints should use "Privacy Grievance". The contact shall be published prominently and supplied in responses concerning personal-data processing.

18.2 STP shall acknowledge grievances within seven working days where practicable and resolve them within 30 calendar days, subject to any shorter applicable legal period. This organizational period is within the operative DPDP rule's maximum of 90 days. Unresolved matters shall be escalated to the Managing Partner without waiting for the deadline to expire.

18.3 Individuals may use applicable statutory complaint and appellate mechanisms, including the Data Protection Board when the relevant provisions apply, after exhausting the required internal grievance opportunity. No confidentiality clause, arbitration provision or Bengaluru jurisdiction clause shall prevent a legally available privacy complaint. Individuals shall provide authentic information, avoid impersonation and refrain from knowingly false or frivolous complaints as required by applicable law.

19.0 Assurance training and governance review

19.1 STP shall train personnel handling personal data, test incident escalation and review processor controls, access rights, retention and response performance. Findings shall have assigned owners and corrective-action dates. High-risk changes shall receive additional review even where a statutory impact assessment is not mandatory.

19.2 The Managing Partner shall review this policy at least annually and after a material legal, operational or security change. Evidence shall include the data register, notices, consent records, contracts, requests, incidents, training and corrective actions. Updates shall be issued with a new effective date and communicated to affected personnel and individuals where required. This policy is governed by Indian law; competent Bengaluru courts apply to matters lawfully within their jurisdiction without excluding statutory authorities or appeals.