Data Privacy Policy

For

Quest2travel India Private Limited

Document Control

Document title	Data Privacy Policy
Classification	Internal — may be shared with clients on request
Applies to	All employees, contractors, trainees and functions of the Company
Status	[Draft / Approved]
Version	1.0
Effective date	1st July 2026
Policy owner	Data Protection Officer
Approved by	[Board]
Prepared by	DPO
Next review	On or before 30th June 2027 or upon material change in law or processing

Contents

Quest2Travel — Data Privacy Policy

Quest2Travel (the **"Company"**, **"we"**, **"us"**) is committed to protecting the privacy of the individuals whose Personal Data it processes, including its employees, customers, corporate clients, travellers, suppliers and website visitors. This Data Privacy Policy (the **"Policy"**) sets out how the Company collects, uses, stores, shares, transfers, retains, protects and erases Personal Data, and how it discharges its accountability as a Data Fiduciary.

This Policy is a core document of the Company's Privacy Information Management System (PIMS), established and maintained in line with ISO/IEC 27701 as an extension to ISO/IEC 27001. It gives effect to the Company's obligations under the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, and supports privacy training, client assurance and continual improvement.

Part A — Purpose, Scope and Framework

1. Purpose

The purpose of this Policy is to define how the Company protects Personal Data throughout its lifecycle, to set out the privacy principles and controls that everyone must follow, and to demonstrate accountability to Data Principals, clients and regulators. It also serves as a reference for employee awareness and training and as a control document within the PIMS.

2. Scope and Applicability

This Policy applies to all Processing of Personal Data carried out by or on behalf of the Company, whether in digital form or in non-digital form that is subsequently digitised, across all locations, systems, devices and media. It applies to all employees, officers, contractors, trainees, interns and third parties who process Personal Data on the Company's behalf. Related policies and procedures operate under and support this Policy.

3. Policy Statement and Commitment

Quest2travel India Pvt. Ltd. is committed to processing Personal Data of its employees, customers, travellers, suppliers and website visitors lawfully, fairly and transparently. We collect only what is necessary and only for clearly defined purposes. We are committed to keeping Personal Data accurate, secure and retain it no longer than required. We believe in honouring the rights of Data Principals; and to embedding privacy by design across our services.

Our leadership endorses this Policy, is committed to provide the resources to implement this Policy, holds Quest2travel accountable for its adherence and continual improvement of this Policy as and when required.

4. Legal and Standards Framework

This Policy is interpreted consistently with, and gives effect to, the following as amended from time to time:

- **DPDP Act and DPDP Rules.** The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, notified in November 2025 and being brought into force in phases up to full operational compliance.
- **Information Technology Act.** The Information Technology Act, 2000 and rules made under it, to the extent applicable.
- **PIMS and security standards.** ISO/IEC 27701, ISO/IEC 27001 and ISO/IEC 27002, which inform the Company's privacy and information security controls.
- **Other applicable laws.** Any other Indian or foreign data protection, sectoral or contractual requirements applicable to the Company's travel and related services.

5. Definitions

Terms used but not defined here have the meaning given under the DPDP Act, the DPDP Rules or, where undefined, their ordinary business meaning.

"Personal Data" means any data about an individual who is identifiable by or in relation to such data.

"Processing" means any operation performed on Personal Data, including collection, storage, use, disclosure, transfer, erasure or destruction.

"Data Principal" means the individual to whom the Personal Data relates, including a parent or lawful guardian of a child and the lawful guardian of a person with a disability.

"Data Fiduciary" means the person who determines the purpose and means of Processing; the Company acts as Data Fiduciary for the data described in this Policy.

"Data Processor" means a person who processes Personal Data on behalf of a Data Fiduciary.

"Consent Manager" means a registered platform through which a Data Principal gives, manages, reviews and withdraws consent.

"Data Protection Board" means the Data Protection Board of India established under the DPDP Act.

"Personal Data Breach" means any unauthorised processing, or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to Personal Data, that compromises its confidentiality, integrity or availability.

"PIMS" means the Company's Privacy Information Management System aligned to ISO/IEC 27701.

"RoPA" means the Records of Processing Activities maintained by the Company.

Part B — Governance, Accountability and Principles

6. Privacy Governance and Roles

Privacy is a shared responsibility supported by clear roles. Quest2travel India Pvt. Ltd. ’s privacy governance comprises:

Role	Key Privacy Responsibilities
Management / Board	Approve the Policy and PIMS, set risk appetite, allocate resources and review performance
Data Protection Officer (DPO)	Own the DPDP Act, PIMS, advise on compliance, handle grievances and liaise with the Data Protection Board
CISO	Implement and monitor technical and organisational security safeguards
Process / data owners	Maintain RoPA entries, retention and lawful basis for their processing
Human Resources	Apply this Policy to employee data and embed privacy in training and onboarding
All employees and contractors	Follow this Policy, complete training and report incidents promptly

7. Accountability and the PIMS

Quest2travel India Pvt. Ltd. demonstrates accountability by maintaining documented policies and procedures, records of processing, risk and impact assessments, training records, incident logs and evidence of control operation. The PIMS is governed through defined objectives, internal audit, management review and continual improvement, so that privacy obligations are not only documented but operating effectively.

8. Privacy Principles

Quest2travel India Pvt. Ltd. applies the following principles to all Processing:

- **Lawfulness, fairness and transparency.** Process only on a lawful basis and tell Data Principals what is happening with their data.
- **Purpose limitation.** Use Personal Data only for the specified, legitimate purposes for which it was collected.
- **Data minimisation.** Collect and retain only what is adequate, relevant and necessary.
- **Accuracy.** Keep Personal Data accurate and up to date.
- **Storage limitation.** Retain Personal Data only as long as necessary, then erase or anonymise it.
- **Integrity and confidentiality.** Protect Personal Data with appropriate security safeguards.
- **Accountability.** Be responsible for, and able to demonstrate, compliance.

Part C — Personal Data, Lawful Basis and Consent

9. Categories of Data Principals and Personal Data

Quest2travel India Pvt. Ltd. processes Personal Data relating to employees and candidates, customers and corporate clients, travellers, suppliers and partners, and website visitors. Categories may include identity and contact data, account and login data, financial and payment data, passport, visa and travel document data, itineraries and travel preferences, statutory identifiers, device and usage data, and welfare or health information where lawfully required. Illustrative records of processing are set out in Schedule 2.

10. Lawful Basis for Processing

Quest2travel India Pvt. Ltd. processes Personal Data only where it has a lawful basis, which may be the consent of the Data Principal or a legitimate use permitted under the DPDP Act, such as Processing necessary for the performance of a contract, for compliance with a legal obligation, or for the purpose for which the Data Principal has voluntarily provided data. The lawful basis for each Processing activity is recorded in the RoPA.

11. Notice and Transparency

Where notice is required, the Company provides a clear, plain-language and itemised notice describing the Personal Data collected, the purposes of Processing, how rights may be exercised, and how consent may be withdrawn and a complaint lodged with the Data Protection Board. Notices are made available in English and, where required, in other languages specified under the DPDP Act.

12. Consent and Consent Management

Where consent is the lawful basis, the Company obtains consent that is free, specific, informed, unconditional and unambiguous, through a clear affirmative action, and records it. Data Principals may withdraw consent at any time with the same ease as giving it, and the Company ceases the relevant Processing within a reasonable time after withdrawal, subject to legal retention requirements. Quest2travel India Pvt. Ltd. may enable consent to be managed through a registered Consent Manager.

Part D — Rights and Duties of Data Principals

13. Rights of Data Principals

Subject to applicable law, Data Principals may exercise the rights to access a summary of their Personal Data and the Processing and sharing of it; to correction, completion and updating of inaccurate or incomplete data; to erasure of data no longer required for its purpose; to grievance redressal; and to nominate another individual to exercise their rights in the event of death or incapacity.

14. Handling Rights Requests

Quest2travel India Pvt. Ltd. operates a defined process to receive, verify, log and respond to rights requests within the timelines prescribed under the DPDP Rules. Requests are authenticated, assessed against any exemptions or legal-hold requirements, actioned across relevant systems and processors, and closed with a response to the Data Principal.

The workflow is set out in Schedule 3.

15. Duties of Data Principals

Data Principals are expected to comply with applicable law when exercising their rights, not to impersonate another person, not to suppress material information where required by law, not to register false or frivolous grievances, and to furnish verifiably authentic information when seeking correction or erasure.

Part E — Privacy by Design, Records and Assessments

16. Privacy by Design and by Default

Privacy and security are considered from the outset of any new process, system, product, vendor engagement or change, and the most privacy-protective configuration applies by default. Data owners engage the DPO and the information security function early so that privacy controls are designed in rather than added afterwards.

17. Records of Processing Activities

Quest2travel India Pvt. Ltd. maintains a RoPA recording, for each Processing activity, the categories of Personal Data and Data Principals, the purposes and lawful basis, recipients and processors, cross-border transfers, retention periods and applicable safeguards. The RoPA is kept current as processing changes and underpins transparency, DPIAs and audits.

18. Data Protection Impact Assessments

Quest2travel India Pvt. Ltd. conducts a Data Protection Impact Assessment for Processing likely to result in high risk to Data Principals, including large-scale processing of sensitive data, new technologies, profiling or significant changes.

The DPIA identifies risks and the measures to mitigate them, and is reviewed by the DPO. Where the Company is designated a Significant Data Fiduciary, it conducts periodic DPIAs and independent audits as required by law.

19. Data Minimisation, Accuracy and Quality

Personal Data is limited to what is necessary, validated for accuracy at the point of collection, and corrected or updated where found to be inaccurate. Free-text and unnecessary fields are avoided, and data quality is monitored for records used to make decisions affecting individuals.

Part F — Security, Access and Monitoring

20. Security Safeguards

Quest2travel India Pvt. Ltd. implements reasonable technical and organisational safeguards to protect Personal Data, which may include encryption, masking or tokenisation, access controls, secure configuration, network and endpoint protection, logging and monitoring with log retention for the period prescribed under the DPDP Rules, secure backups and tested recovery. Safeguards are aligned to the Company's ISO/IEC 27001 controls and reviewed periodically.

21. Access Control and Acceptable Use

Access to Personal Data and systems is granted on a need-to-know and least-privilege basis, governed by joiner-mover-leaver processes and periodic access reviews. Users authenticate with individual credentials and multi-factor authentication where required, and use Company systems only for legitimate business purposes in line with the acceptable use and classification policies.

22. Monitoring

To the extent permitted by law and for security, compliance and legitimate operational purposes, the Company may monitor the use of its systems, communications, networks and facilities. Monitoring is proportionate, governed by policy, and conducted with appropriate transparency to those affected.

Part G — Third Parties, Transfers and Retention

23. Processors, Sub-Processors and Third Parties

Quest2travel India Pvt. Ltd. shares Personal Data with processors and partners — such as payroll and HRMS providers, airlines, hotels, global distribution systems, payment providers, insurers, auditors and verification agencies — only on a need-to-know basis and under contracts containing data protection obligations. Processors are subject to due diligence, must implement appropriate safeguards, and may engage sub-processors only with authorisation and equivalent protections.

24. Cross-Border Transfers

Quest2travel India Pvt. Ltd. may transfer or store Personal Data outside India where permitted under the DPDP Act and the DPDP Rules, which allow such transfers except to countries or territories specifically restricted by the Central Government. Transfers are subject to appropriate contractual, organisational and technical safeguards, and cross-border flows are recorded in the RoPA.

25. Data Retention and Erasure

Personal Data is retained only for as long as necessary to fulfil its purpose or to meet contractual, statutory or regulatory requirements, after which it is securely erased or anonymised. Erasure is carried out where the purpose is served, consent is withdrawn or a retention period expires, in accordance with the timelines prescribed under the DPDP Rules. Quest2travel India Pvt. Ltd. maintains a retention schedule and applies legal holds where data must be preserved.

Part H — Breach, Children, Training and Assurance

26. Personal Data Breach Management

Quest2travel India Pvt. Ltd. operates an incident response process to detect, contain, assess, remediate and learn from Personal Data Breaches. On becoming aware of a breach, the Company intimates affected Data Principals and reports to the Data Protection Board within the timelines prescribed under the DPDP Rules, which require a report to the Board within seventy-two hours. All personnel must report suspected breaches immediately through the incident channel; breach response steps are summarised in Schedule 4.

27. Children's and Vulnerable Persons' Data

Where the Company processes the Personal Data of a child or a person with a disability who has a lawful guardian, it obtains verifiable consent from the parent or lawful guardian as required by law, and does not undertake processing likely to cause detriment to a child, tracking, behavioural monitoring or targeted advertising directed at children, except as permitted under the DPDP Rules.

28. Privacy and Security Training and Awareness

All personnel complete privacy and security awareness training on joining and periodically thereafter, with role-specific training for those handling sensitive or large volumes of Personal Data. Training records are retained as evidence of accountability, and awareness is reinforced through communications and policy updates.

Part I — Compliance, Review and Contacts

29. Grievance Redressal and Privacy Contacts

Data Principals may contact the Company's Data Protection Officer or Grievance Officer for any privacy request, query or complaint. Quest2travel India Pvt. Ltd. maintains an effective grievance mechanism and responds within the prescribed period; unresolved grievances may be escalated to the Data Protection Board of India.

Data Protection Officer	
Email	[privacy@quest2travel.com]
Postal address	6th Floor, A Wing, Mumbai Educational Trust (MET, General Arun Kumar Vaidya Marg, opposite Lilavati Hospital, Reclamation, Bandra West, Mumbai, Maharashtra 400050
Escalation	Data Protection Board of India

30. Internal Audit, Monitoring and Management Review

Quest2travel India Pvt. Ltd. monitors the effectiveness of its privacy controls through metrics, internal audits and assessments, and reviews PIMS performance at management reviews. Findings drive corrective action and improvement.

31. Continual Improvement and Document Control

This Policy and related PIMS documents are version-controlled, with defined owners, approval and review cycles. Quest2travel India Pvt. Ltd. continually improves its privacy programme in response to audit findings, incidents, regulatory change and stakeholder feedback.

32. Compliance, Non-Compliance and Disciplinary Action

Compliance with this Policy is mandatory. Breach of this Policy may result in disciplinary action up to and including termination of employment or contract, and may also expose individuals and the Company to legal consequences, including significant penalties under the DPDP Act for the Company.

33. Review of this Policy

This Policy is reviewed at least annually and whenever there is a material change in law, regulation, the Company's processing or its PIMS. The current approved version supersedes all earlier versions.

Schedule 1 — Roles and Responsibilities

Activity	Responsible	Accountable
Approve Policy and PIMS	DPO	Management / Board
Maintain RoPA	Data owners	DPO
Operate security safeguards	Information security	DPO / CISO
Handle rights requests	DPO / function	DPO
Breach reporting	Incident team	DPO / CISO
Training delivery	HR / DPO	DPO

Schedule 2 — Illustrative Records of Processing

Illustrative only; the live RoPA is maintained separately.

Activity	Data Category	Lawful Basis	Indicative Retention
Employee administration	Identity, payroll, statutory	Contract / legal obligation	Employment + statutory period
Travel booking	Traveller, passport, itinerary	Contract / legitimate use	Service + contractual period
Payments	Billing and payment data	Contract / legal obligation	As required by law
Website and accounts	Contact, login, usage	Consent / legitimate use	Until withdrawal or inactivity
Vendor management	Supplier contact data	Contract	Contract term + statutory period

Schedule 3 — Data Subject Rights Request Workflow

Step	Action
1. Receive	Capture the request through the privacy channel and log it
2. Verify	Authenticate the identity of the requester
3. Assess	Determine the right requested, scope, exemptions and legal holds
4. Action	Retrieve, correct, erase or compile data across systems and processors
5. Respond	Provide the response within the prescribed timeline and close the log
6. Improve	Review recurring requests for process improvement

Schedule 4 — Personal Data Breach Response Steps

Step	Action
1. Report	Anyone aware of a suspected breach reports it immediately via the incident channel to CISO/DPO
2. Contain	Limit further exposure and preserve evidence
3. Assess	Determine scope, data and individuals affected and likely impact
4. Notify	Intimate affected Data Principals and report to the Data Protection Board within 72 hours
5. Remediate	Fix root cause and recover affected systems and data
6. Review	Conduct a post-incident review and update controls

Schedule 5 — Key Definitions Quick Reference

Term	Plain-Language Meaning
Data Principal	The individual the Personal Data is about
Data Fiduciary	The organisation that decides why and how data is processed (the Company)
Data Processor	A party that processes data on the Company's behalf
Consent Manager	A registered platform to manage and withdraw consent
Data Protection Board	The authority that oversees compliance and complaints
RoPA	Quest2travel India Pvt. Ltd. 's records of processing activities
PIMS	Privacy Information Management System aligned to ISO/IEC 27701