

39 DEGREES SOUTH

Privacy Policy

Tour Operations | Travel Services | Experiential Tourism

Effective Date: 22 February 2026 | Version 1.0

Applicable Frameworks: Australian Privacy Act 1988 (Cth) | GDPR (EU/UK) | CCPA (California)

1. Introduction and Overview

39 Degrees South Pty Ltd (ABN 4716222273) ('39 Degrees South', 'we', 'us', or 'our') is a licensed Australian tour operator providing curated travel, adventure, and experiential tourism services to travellers to/from Australia and around the world. In delivering these services, we necessarily collect, hold, use, and disclose personal information — including sensitive information such as health and medical details and government-issued identity documents — to arrange safe, personalised, and legally compliant travel experiences.

This Privacy Policy explains how we manage personal information in accordance with our obligations under:

- the Privacy Act 1988 (Cth) ('Privacy Act') and the Australian Privacy Principles ('APPs'), as amended by the Privacy and Other Legislation Amendment Act 2024;
- the General Data Protection Regulation (EU) 2016/679 ('GDPR') and the UK GDPR, where applicable to travellers from the European Economic Area or the United Kingdom;
- the California Consumer Privacy Act 2018 ('CCPA'), as amended by the California Privacy Rights Act ('CPRA'), where applicable to California residents.

We also collaborate with a specialist cybersecurity partner based in the United States of America ("StrongAuth Inc" dba StrongKey) to provide our business customers (such as travel agents, corporate travel managers, and group organisers) with a secure platform for transmitting their clients' Personally Identifiable Information ('PII') to us. This Policy addresses how personal information is handled across all aspects of our operations.

By engaging our services, using our website, or providing us with personal information, you acknowledge that you have read and understood this Privacy Policy.

2. About 39 Degrees South

39 Degrees South is an Australian-based tour operator specialising in tours for wilderness expeditions, cultural immersion tours, sports & adventure travel, eco-tourism, and multi-day trekking experiences across Australia and internationally. Our clients include individual travellers, groups, corporate clients, and international visitors, many of whom book through travel agencies or group booking platforms.

As a tour operator, we routinely handle sensitive categories of personal information — including health and medical information relevant to physical participation in tours, dietary

requirements, and emergency contact details — as well as government-issued identity documents required for travel bookings and compliance purposes.

Registered address: 1/267 A Glenferrie Road, Malvern, VIC 3144, Australia

Privacy Officer: N. Noor | Email: info@39degreessouth.com.au | Phone: [03 59180809]

3. Personal Information We Collect

We collect personal information that is reasonably necessary to provide our tour services, comply with legal obligations, and ensure the safety of all participants. The types of personal information we collect include:

3.1 Identity and Contact Information

- Full legal name (as it appears on government-issued ID)
- Date of birth
- Residential and postal addresses
- Email addresses and phone numbers
- Emergency contact details (name, relationship, phone number)

3.2 Government-Issued Identity Documents

For the purposes of tour bookings, travel compliance, visa applications, park permits, and insurance, we collect:

- Passport number, expiry date, and country of issue
- Driver's licence number and state/country of issue (where required for driving activities)
- National identity card details (where applicable)
- Visa and immigration documents (where required for international tours)

We treat government ID information with the highest level of care and restrict access to it on a strict need-to-know basis.

3.3 Health and Medical Information

As a tour operator offering physical, outdoor, and adventure activities, the collection of health information is essential to participant safety and is a legitimate purpose under the Privacy Act and GDPR. We collect:

- Pre-existing medical conditions relevant to tour participation (e.g., heart conditions, epilepsy, respiratory conditions)
- Physical fitness information and mobility limitations
- Dietary requirements and food allergies (including life-threatening allergies)
- Medications being taken, where relevant to emergency medical response
- Disability-related information required to provide reasonable adjustments
- Vaccination status (where required for international destinations or government permit conditions)

We collect health information only to the extent necessary for participant safety, insurance purposes, and legal compliance. We will always seek your explicit consent before collecting health information, and you have the right to refuse, though this may affect your ability to participate in certain activities.

3.4 Payment and Financial Information

- Credit/debit card details (processed via PCI-DSS compliant third-party payment gateways — we do not store full card numbers)
- Bank account details for refunds
- Travel insurance policy details

3.5 Technical and Usage Information

- IP address, browser type, and device identifiers
- Website navigation and booking platform interactions
- Cookies and analytics data (see Section 14)

3.6 Information Submitted via Our Secure Platform (Agent/Operator Submissions)

When travel agents, group organisers, or corporate clients submit client PII through our secure transmission platform (facilitated by our US Cybersecurity Partner), this may include any of the above categories on behalf of their clients. Our business customers are responsible for ensuring their clients have been informed and, where required, have consented to the submission of their personal information to 39 Degrees South.

4. How We Collect Personal Information

We collect personal information through the following means:

- Directly from travellers via online booking forms, enquiry forms, and registration processes
- From travel agents, group leaders, or corporate booking managers acting on behalf of travellers
- Via our secure PII transmission platform, where agents submit traveller details
- Through email, telephone, or in-person communications
- From our website, mobile applications, and booking systems
- From third parties, including insurance providers, tour partner operators, and accommodation providers
- Automatically via cookies, server logs, and analytics tools

Where practicable, we will inform you at the point of collection why we are collecting your personal information and how it will be used. We will only collect sensitive information (such as health and government ID information) with your explicit consent, except where permitted by law.

5. How We Use Personal Information

We use personal information for the following purposes:

5.1 Tour Operations and Safety

- Booking, reserving, and confirming tour places and accommodation
- Assessing participant suitability and managing health and safety requirements
- Providing necessary medical information to guides, first aiders, or emergency services
- Obtaining permits, visas, and insurance on behalf of travellers

- Communicating pre-departure information, itinerary changes, and emergency alerts

5.2 Identity Verification and Compliance

- Verifying traveller identity in accordance with tour permit conditions
- Complying with airline, border control, or national park authority requirements
- Meeting Australian and international anti-money laundering and counter-terrorism financing obligations

5.3 Business Administration

- Processing payments and managing refunds or cancellations
- Managing agent and corporate customer accounts
- Customer service and complaint resolution
- Marketing our services to existing and prospective clients (with consent where required)
- Improving our website, booking systems, and service delivery

5.4 Legal Obligations

We may use personal information to comply with applicable laws and regulations, to respond to lawful requests from government authorities, and to protect the rights, property, and safety of 39 Degrees South, our staff, and our travellers.

6. Legal Basis for Processing (GDPR and UK GDPR)

For travellers from the European Economic Area (EEA) or the United Kingdom, we process personal information on the following legal bases under Article 6 of the GDPR:

- Contract: processing is necessary to perform the travel services contract (e.g., booking tours, arranging permits and accommodation)
- Legal obligation: processing is required to comply with applicable laws (e.g., customs and immigration requirements, workplace health and safety laws)
- Vital interests: processing is necessary to protect the vital interests of a traveller (e.g., providing health information to emergency services)
- Legitimate interests: processing is necessary for our legitimate business interests, such as fraud prevention, marketing to past customers, and improving our services, where these interests are not overridden by your rights
- Consent: for processing that is not otherwise justified on the above grounds, including collecting sensitive personal data such as health information and government IDs, and sending direct marketing communications

For special categories of data (including health information) under Article 9 of the GDPR, we rely on:

- Explicit consent (Article 9(2)(a))
- Processing necessary for the purposes of preventive or occupational medicine, assessment of working capacity, or management of health systems (Article 9(2)(h))
- Processing necessary to protect the vital interests of the data subject (Article 9(2)(c))

EEA and UK individuals also have enhanced data subject rights as set out in Section 11 below.

7. California Consumer Privacy Act (CCPA / CPRA)

If you are a California resident, this section supplements the rest of our Privacy Policy and describes your rights under the California Consumer Privacy Act 2018, as amended by the California Privacy Rights Act 2020 ('CCPA/CPRA').

7.1 Categories of Personal Information Collected

In the preceding 12 months, we have collected the following categories of personal information from California consumers:

- Identifiers (names, email addresses, passport numbers, driver's licence numbers)
- Protected classification characteristics (health/medical information, disability status)
- Commercial information (booking and transaction records)
- Internet or other network activity (website interaction data)
- Geolocation data (where used during tours with tracking features, with consent)
- Sensitive personal information (government ID, health information, financial account data)

7.2 Your CCPA/CPRA Rights

California residents have the following rights, subject to certain exceptions:

- Right to Know: you may request details of the categories and specific pieces of personal information we have collected about you and how it has been used and disclosed
- Right to Delete: you may request deletion of your personal information, subject to exceptions (e.g., where we are required to retain it by law)
- Right to Correct: you may request correction of inaccurate personal information
- Right to Opt-Out of Sale or Sharing: we do not sell or share personal information for cross-context behavioural advertising within the meaning of the CCPA
- Right to Limit Use of Sensitive Personal Information: you may request that we limit our use of sensitive personal information to purposes permitted by the CPRA
- Right to Non-Discrimination: we will not discriminate against you for exercising your CCPA/CPRA rights

To exercise your California privacy rights, please contact us using the details in Section 15. We will respond to verifiable consumer requests within 45 days, with a possible 45-day extension where reasonably necessary.

8. Disclosure of Personal Information

We may disclose personal information to the following third parties:

- Our US Cybersecurity Partner —StrongKey, for the purpose of facilitating secure PII transmission (see Section 9)
- Tour guides, ground operators, and activity providers — necessary for tour delivery and participant safety
- Accommodation and transport providers — for booking and logistical purposes
- Insurance providers — to obtain or administer travel and tour insurance
- Government and regulatory authorities — including parks, border control, visa agencies, and permit issuers
- Emergency services — including hospitals, paramedics, or search and rescue, where required for participant safety

- Payment processors — PCI-DSS compliant providers who process tour payments
- Marketing and analytics platforms — only aggregated or de-identified data where possible
- Professional advisors — lawyers, accountants, and auditors bound by confidentiality obligations

We do not sell personal information to third parties. We do not share health or government ID information with any party except as strictly necessary for the tour operation, participant safety, or legal compliance.

9. Cross-Border Disclosure and International Transfers

Given the nature of our tour operations and our cybersecurity partnership arrangement, personal information may be transferred and processed outside Australia. We take these transfers seriously and ensure appropriate safeguards are in place.

9.1 Transfer to US Cybersecurity Partner (APP 8 Compliance)

Consistent with Australian Privacy Principle 8 and the 2024 amendments to the Privacy Act, we have taken the following steps in respect of the cross-border disclosure of personal information to our US Cybersecurity Partner:

- We have entered into a comprehensive Data Processing Agreement ('DPA') requiring the Partner to handle all personal information consistently with the Australian Privacy Principles
- The DPA prohibits the Partner from using personal information for any purpose other than providing agreed cybersecurity and secure transmission services
- The Partner is required to implement technical and organisational security measures meeting or exceeding industry standards (including SOC 2 Type II and ISO 27001)
- The Partner must notify us immediately upon becoming aware of any actual or suspected breach involving personal information
- We retain accountability under section 16C of the Privacy Act for the Partner's handling of personal information

9.2 International Tour Operations (GDPR Chapter V)

For travellers from the EEA or UK whose data is shared with tour operators or service providers outside the EEA/UK (including within Australia), we ensure transfers are conducted in accordance with GDPR Chapter V, relying on:

- Adequacy decisions where applicable
- Standard Contractual Clauses (SCCs) adopted by the European Commission
- Derogations under Article 49 GDPR where applicable (e.g., transfer necessary for the performance of a contract entered into in the interest of the data subject)

9.3 Other International Transfers

In operating tours across multiple countries, traveller information (particularly passport details and emergency contact information) may be shared with foreign government authorities, accommodation providers, and ground operators in the destination country. This sharing is necessary for the performance of the tour contract and for the safety of participants. We will inform you of significant international data flows at the time of booking.

10. How We Protect Your Information

We implement comprehensive technical and organisational security measures to protect personal information — including sensitive health data and government identity documents — from misuse, interference, loss, unauthorised access, modification, and disclosure. Our security measures include:

- End-to-end encryption (AES-256 or equivalent) for all PII transmitted through our secure platform
- SSL/TLS encryption for all data transmitted via our website and booking systems
- Multi-factor authentication for all staff accessing personal information
- Role-based access controls — health and government ID information is accessible only to authorised staff on a strict need-to-know basis
- Encrypted storage for all sensitive data at rest
- Regular security audits, penetration testing, and vulnerability assessments
- Staff training on privacy and data protection obligations
- Physical security controls at our offices
- Incident response procedures, including immediate breach containment and notification protocols

Despite our best efforts, no system is entirely secure. In the event of an eligible data breach as defined under the Notifiable Data Breaches scheme (Part IIIC of the Privacy Act), we will notify the Office of the Australian Information Commissioner and affected individuals as soon as practicable. For EEA/UK individuals, we will notify the relevant supervisory authority within 72 hours of becoming aware of a breach, where required by the GDPR.

11. Your Privacy Rights

11.1 Australian Privacy Rights (APPs)

Under the Privacy Act, you have the right to:

- Access the personal information we hold about you (APP 12) — we will respond within 30 days
- Request correction of inaccurate, out-of-date, incomplete, or misleading information (APP 13)
- Lodge a complaint with us regarding our handling of your personal information, and to escalate to the OAIC if unresolved
- Opt out of direct marketing communications at any time

11.2 GDPR and UK GDPR Rights (EEA/UK Travellers)

In addition to the above, EEA and UK residents have the following rights under the GDPR:

- Right of access (Article 15): obtain a copy of your personal data and information about how it is processed
- Right to rectification (Article 16): have inaccurate personal data corrected
- Right to erasure / 'right to be forgotten' (Article 17): request deletion of your personal data in certain circumstances
- Right to restriction of processing (Article 18): request that we limit how we process your data in certain circumstances
- Right to data portability (Article 20): receive your data in a structured, machine-readable format

- Right to object (Article 21): object to processing based on legitimate interests or for direct marketing
- Right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before withdrawal
- Right to lodge a complaint with your local supervisory authority (e.g., the ICO in the UK, or your national DPA in the EU)

11.3 Health Information — Special Considerations

Where you provide health information for the purpose of tour participation, you may withdraw consent at any time. However, please note that withdrawal of consent to process health information may mean we are unable to safely accommodate you on certain tours. We will discuss alternative arrangements with you in that event.

12. Data Retention

We retain personal information for as long as necessary to fulfil the purposes described in this Policy or as required by law. Retention periods include:

- Booking and tour records (including identity documents): 7 years after the tour date, to satisfy tax, insurance, and legal obligations
- Health and medical information: retained for the duration of the tour and for a reasonable period thereafter for insurance and legal purposes (typically 7 years), then securely destroyed
- Payment records: 7 years in accordance with Australian tax law
- Incident and emergency records: retained as long as required by applicable law or pending resolution of any claim
- Marketing contact lists: until you opt out or request removal

When personal information is no longer required, we securely destroy, delete, or permanently de-identify it. We also require our US Cybersecurity Partner and other processors to return or destroy personal information upon termination of their engagement.

13. Children's Privacy

Some of our tours accommodate families with children. Where we collect personal information about minors (under 18 years of age), including health information and identity documents for tour registration, we collect this information from a parent or legal guardian. We will seek explicit consent from a parent or guardian for the collection of a minor's sensitive personal information.

Parents or guardians may request access to, correction of, or deletion of personal information held about their child by contacting us using the details in Section 15.

14. Cookies and Online Tracking

Our website and booking platform use cookies and similar tracking technologies to improve functionality and understand how visitors interact with our services. We use:

- Essential cookies: required for core website and booking functionality; these cannot be disabled
- Analytical cookies: help us understand visitor behaviour and improve our platform (e.g., Google Analytics — anonymised where possible)

- Functional cookies: remember your preferences to provide a personalised experience

You may manage or disable non-essential cookies through your browser settings or our cookie consent tool. For EEA/UK visitors, we obtain consent for non-essential cookies in accordance with the GDPR and applicable ePrivacy rules before placing them on your device.

15. Contact Us and Exercising Your Rights

To exercise any of your privacy rights, lodge a complaint, or raise any privacy concerns, please contact our Privacy Officer:

39 Degrees South — Privacy Officer

Name: N. Noor

Email: info@39degreessouth.com.au

Phone: [03 59180809]

Address: 1/267 A Glenferrie Road, Malvern, VIC 3144, Australia

We aim to acknowledge all privacy requests within 5 business days and will endeavour to resolve them within 30 days (or within 45 days for CCPA requests). Where we are unable to meet these timeframes, we will notify you of the delay and the expected resolution date.

If you are not satisfied with our response, you may escalate your complaint to:

- Office of the Australian Information Commissioner (OAIC): www.oaic.gov.au | 1300 363 992
- UK Information Commissioner's Office (ICO): www.ico.org.uk | 0303 123 1113
- Your national EU Data Protection Authority: edpb.europa.eu/about-edpb/board/members_en
- California Privacy Protection Agency (CPPA): cppa.ca.gov

16. Updates to This Privacy Policy

We may update this Privacy Policy from time to time. When we make material changes, we will notify you by email (for existing customers) and/or by posting a prominent notice on our website at least 14 days before the changes take effect. Continued use of our services after the effective date of a revised Policy constitutes your acceptance of the updated Policy.

The current version of this Policy is available at [www.39degreessouth.com.au/privacy] and will always display the effective date and version number.

17. Governing Law

This Privacy Policy is governed by the laws of Victoria, Australia. Nothing in this Policy limits rights that individuals may have under applicable international privacy laws (including the GDPR or CCPA), which apply independently of this Policy to the extent they are applicable to 39 Degrees South's processing activities.