CUSTOMER PRIVACY & PERSONAL DATA PROTECTION POLICY

1. PURPOSE & SCOPE

SiamRise Travel respects the privacy of all customers, employees, and business partners.

This policy covers how we collect, store, use, share, and delete personal data. We comply with the Constitution of the Kingdom of Thailand B.E. 2560 (2017), the Personal Data Protection Act (PDPA) B.E. 2562 (2019), and other relevant laws, including the Electronic Transactions Act B.E. 2544 (2001).

2. LEGAL STATUS & ROLES

Under the Thai PDPA, SiamRise Travel may act as both a Data Controller and a Data Processor, depending on the activity.

We collect and process personal data only for lawful and necessary purposes, such as providing travel services, managing bookings, communicating with customers, and arranging required travel insurance.

3. DATA COLLECTION & EXPLICIT CONSENT

- Necessity Principle: We only collect personal data, such as full name, contact details, passport number, and nationality, when it is necessary to provide our services. Sensitive personal data, such as dietary requirements, health information, or religion, is only collected when necessary for specific travel arrangements and with appropriate consent or legal basis.

- Purpose Notification: Customers are informed about why their personal data is being collected at the time of booking. If the purpose of processing changes, customers will be informed and, where required, asked to provide new consent.

- Consent Withdrawal and Data Rights: Customers have the right to withdraw consent and may request access, correction, deletion, or anonymization of their personal data, subject to applicable law. Requests can be made by contacting booking@siamrisetravel.com.

4. DATA RETENTION PERIOD (MAXIMUM 1 YEAR)

In line with our internal data protection and sustainability standards:

- All personal data and customer information are kept for a maximum of one (1) year after completion of the booked travel service, unless a longer period is required by law.

- After this period or following a verified customer request for deletion where applicable, digital records will be securely deleted or anonymized. Physical documents containing personal data will be securely shredded before disposal.

5. DATA SECURITY, ACCESS CONTROL & STORAGE

- Electronic Storage: Personal and sensitive information is stored in password-protected and, where applicable, encrypted systems. Access is limited to authorized and trained staff who are required to maintain confidentiality.

- Physical Storage: Printed documents containing personal data are kept in locked filing cabinets at our office and are accessible only to authorized employees.

- Third-Party Sharing: Personal data is shared only when necessary with trusted operational suppliers, such as hotels, transport providers, local guides, and travel insurance providers, to deliver the agreed travel services. Personal data is never sold, rented, or traded to third parties.

6. INCIDENT MANAGEMENT AND DATA BREACH NOTIFICATION

SiamRise Travel maintains appropriate records and procedures for managing personal data and responding to data breaches.

In the event of a suspected or confirmed personal data breach:
Step 1 – Containment & Assessment:
The responsible person immediately secures the affected systems, restricts access, and assesses the scope and potential impact of the incident.

Step 2 – Official Notification:
SiamRise Travel will notify the Personal Data Protection Committee (PDPC) and affected data subjects within the period required by Thai law, where notification is required.

Step 3 – Corrective Action & Logging:
Corrective actions will be taken as soon as possible to reduce the impact and prevent the incident from happening again. Details of the incident and actions taken will be recorded in our internal data breach log.

Thanawut S.

(Thanawut Supangkaratana)
Sustainability Coordinator

Piyapun S.

(Piyapun Supangkaratana)
General Manager