

Privacy Policy and Handling of Personal Information

1. Privacy Policy

RESPECT PAYMENT SERVICE Co., Ltd. (the “Company”) recognizes the importance of personal information and user information handled in its funds transfer business and other services, and complies with the Act on the Protection of Personal Information (APPI), other applicable laws and regulations, guidelines and internal policies.

The Company collects personal information by lawful and fair means and processes it only to the extent necessary to achieve purposes of use specified and disclosed or notified in advance.

The Company implements necessary and appropriate organizational, personnel, physical and technical security measures to prevent leakage, loss, damage, unauthorized access, use outside stated purposes and other improper handling of personal information.

When entrusting the processing of personal data to third parties, the Company appropriately selects and supervises contractors by entering into agreements, reviewing processing practices and other measures.

The Company continuously trains officers and employees on personal information protection and information security.

The Company responds appropriately to inquiries, consultations, complaints and disclosure-related requests from individuals under applicable laws and prescribed procedures.

The Company periodically reviews its personal information management framework and continually improves it in response to changes in social conditions, laws, technology and business activities.

2. Name of the Company

RESPECT PAYMENT SERVICE Co., Ltd.

3. Privacy Management Officer

The Company appoints a privacy management officer to ensure the proper management of personal information.

The role, contact methods and other necessary particulars of this officer are managed under the Company’s internal framework and through its inquiry desk.

4. Personal Information Collected

The Company may collect the following personal information for service provision, identification, legal compliance and customer support:

(1) Name, former name, commonly used name and other identifying information

(2) Date of birth, gender, nationality or region

(3) Address, telephone number, email address and other contact information

(4) Occupation, employer, business activities and other attributes

(5) Residence status, authorized period of stay and related information

(6) Information and images appearing on identification documents

(7) Facial images, biometric authentication data and other information required for identity verification

- (8) Bank accounts, deposit accounts, beneficiary accounts, wallets and other payment or funds transfer information
- (9) Remitter and beneficiary information, amount, purpose, source of funds, relationship to beneficiary and other transaction details
- (10) Service use, remittance, payment, deposit, withdrawal, cancellation, recall and refund records
- (11) Customer risk assessment, transaction review and legal compliance information
- (12) Inquiries, consultations, complaints and dispute-handling information
- (13) Device data, IP address, login records, operation logs, location information and other technical service usage data
- (14) Call recordings, email, chat and other communications with the Company
- (15) Campaign and survey applications or responses
- (16) Information on representatives, officers of corporate customers, beneficial owners and other related persons
- (17) Other information necessary for providing services and complying with law

5. Methods of Collection

The Company collects personal information by the following and other lawful and fair methods:

- (1) Applications and other written documents
- (2) The Company's website, app and other electronic channels
- (3) Identification documents, facial images and other identity verification procedures
- (4) Telephone, email, chat and in-person communications
- (5) Information obtained from banks, payment collection institutions, remittance destinations, overseas partners and other related businesses
- (6) Information lawfully and contractually obtained from contractors and other third parties
- (7) Access logs, device data and other technical data automatically generated by use of the services

6. Purposes of Use

The Company uses collected personal information for the following purposes:

- (1) Service applications, registration and contracting
- (2) Identity and transaction verification, verification of agency authority, and updates to customer information
- (3) Provision of international remittances and other funds transfer services
- (4) Processing deposits, remittances, receipt of funds, cancellations, recalls and refunds
- (5) Coordination with remittance destinations, financial institutions, collection institutions, overseas partners and other parties
- (6) Notifications regarding remittance status, service use and other service matters
- (7) Display or notification of fees, exchange rates, expected amounts receivable and other transaction terms

- (8) Prevention of transfer of criminal proceeds, money laundering, terrorist financing and proliferation financing
- (9) Economic sanctions checks and checks required by the Foreign Exchange and Foreign Trade Act or other laws
- (10) Customer risk assessment, transaction monitoring and review of suspicious or abnormal transactions
- (11) Filing suspicious transaction reports and other mandatory filings or reports
- (12) Prevention, detection and investigation of unauthorized use, impersonation, fraudulent transfers, fraud and other crime or misconduct
- (13) Protection of account and service security
- (14) Handling customer inquiries, complaints, compensation claims and disputes
- (15) Responses to incidents, system outages and information security events
- (16) Maintaining, improving and controlling service quality and considering new services
- (17) Preparing statistical, analytical and other materials in a form that does not identify individuals
- (18) Notification of changes in terms, important information, policies, fees and other matters
- (19) Exercising the Company's rights and performing its obligations
- (20) Audits, accounting, tax, legal matters, compliance and internal controls
- (21) Responses to requests from courts, police, supervisory authorities and other public bodies under law
- (22) Other purposes incidental or related to those above

7. Sensitive Personal Information

When acquiring special care-required personal information, the Company obtains the individual's prior consent unless otherwise permitted by law.

Images of identification documents, facial images, biometric authentication data and other information requiring particular care are used only as needed for identity verification, prevention of impersonation, legal compliance and other specified purposes.

Access to such information is restricted to personnel who need it for their work and it is managed more stringently than ordinary personal information.

8. Changes to Purposes of Use

The Company may change a purpose of use to the extent that the change is reasonably related to the original purpose.

If a purpose of use changes, the Company notifies individuals or publishes the revised purpose on its website or by other appropriate means.

9. Accuracy of Personal Data

The Company endeavors to keep personal data accurate and up to date to the extent necessary to achieve the purposes of use.

Customers must notify the Company of changes to their registered information in the manner designated by the Company.

10. Retention Periods

The Company retains personal data for periods necessary in light of laws, regulatory requirements, contracts, the nature of transactions, statutory record-retention obligations, complaints, disputes and incidents.

Personal data no longer required will be securely deleted or disposed of in accordance with applicable law and internal policies.

11. Disclosure of Personal Data to Third Parties

The Company does not disclose personal data to third parties without the individual's consent except in the following cases:

- (1) Where required by law
- (2) Where necessary to protect life, body or property and obtaining consent is difficult
- (3) Where particularly necessary for public health or the sound development of children and obtaining consent is difficult
- (4) Where cooperation is necessary for the performance of statutory duties by national or local governments or their delegates and obtaining consent might impede those duties
- (5) Disclosure for academic research or other cases permitted by law
- (6) Other cases that do not constitute a third-party disclosure under law

Where personal data is disclosed to or received from a third party, the Company undertakes the verification and recordkeeping required by applicable law.

12. Information Shared in the Course of Remittances

The Company may share information necessary to execute customer-requested international remittances with remittance partners, receiving financial institutions and other relevant parties. In ordinary remittance messages, the personally identifying information concerning the remitter and beneficiary consists of names and cities.

- (1) Remitter's name and city
- (2) Beneficiary's name and city
- (3) Transaction details needed for remittance processing, including amount, currency and transaction reference number
- (4) Information needed for cancellation, recall or confirmation of payment
- (5) Information whose necessity and lawfulness have been reviewed individually for legal inquiries, sanctions checks or investigations into unauthorized use

As part of ordinary payment instructions, the Company does not automatically disclose images of identification documents collected in Japan, full residential addresses or dates of birth. The information transmitted abroad may, however, vary according to the transaction message or an individual lawful request. Disclosures are limited to what is necessary for remittance processing, legal compliance and fraud prevention.

13. Disclosure to Third Parties in Foreign Countries

The Company may disclose personal data to overseas remittance partners, financial institutions, wallet operators and other relevant parties as necessary for international remittance services.

In accordance with Articles 27 and 28 of the APPI and other applicable provisions, the Company obtains consent where legally required or takes other measures permitted by law.

(1) Obtaining consent for overseas disclosure after providing information legally required in advance

(2) Where the overseas recipient has established a system ensuring continuous implementation of measures equivalent to those required of Japanese personal information handling businesses, applying the legally required safeguards

(3) Other means of transfer permitted under the APPI

Where relying on consent, the Company provides legally required information in advance concerning the recipient's country, the personal information protection system in that country and measures taken by the recipient. Where relying on equivalent safeguards, the Company conducts ongoing verification and other legally required measures and responds to statutory requests for information.

Schedule 1 describes the principal recipient countries, categories of recipients, information disclosed and purposes. The mere fact that information is transmitted pursuant to a customer's remittance request does not automatically remove the applicability of Article 28 of the APPI.

14. Outsourcing of Personal Data Processing

The Company may outsource all or part of the processing of personal data within the scope necessary for the purposes of use.

The Company appropriately selects processors and uses contracts or other measures to manage the following:

(1) Confidentiality

(2) Processing only for specified purposes

(3) Security controls

(4) Access permissions

(5) Subcontracting

(6) Reporting of incidents and data breaches

(7) Company oversight, checks and audits

(8) Return, deletion or destruction on contract expiry

(9) Other measures needed for secure personal data processing

15. Joint Use of Personal Data

Where the Company jointly uses personal data with specified parties, it provides advance notice or makes readily accessible information on:

(1) The fact of joint use

(2) The items of personal data jointly used

(3) The scope of joint users

(4) The purposes of joint use

(5) The name, address and representative of the party responsible for management of the jointly used data

16. Security Management Measures

To prevent leakage, loss, damage, misuse or unauthorized access, the Company employs the following safeguards:

Organizational safeguards

- (1) Appointment of a privacy officer and other responsible personnel
- (2) Establishment of handling policies and procedures
- (3) Monitoring and recording of processing
- (4) Incident reporting and response arrangements
- (5) Regular self-assessments and internal audits

Personnel safeguards

- (1) Confidentiality obligations for officers and employees
- (2) Information management on hiring and departure
- (3) Regular education and training
- (4) Reporting and correcting non-compliance

Physical safeguards

- (1) Management of offices and storage areas
- (2) Locked storage of paper documents, devices and media
- (3) Prevention of theft or loss of devices and media
- (4) Secure transport, return and disposal of personal data

Technical safeguards

- (1) User and access-rights management
- (2) Authentication and prevention of unauthorized access
- (3) Protection of transmitted and stored data
- (4) Logging and monitoring
- (5) Protection from malware, vulnerabilities and cyberattacks
- (6) Backup and recovery
- (7) Security management of cloud and other external services

17. Processing Personal Data Overseas

Where the Company processes personal data overseas or uses overseas contractors or services, it assesses the data protection laws and other circumstances of the relevant country or region and implements safeguards appropriate to those circumstances.

18. Response to Personal Data Breaches

If the Company becomes aware of a breach, loss, destruction or similar incident involving personal data or a risk thereof, it promptly undertakes:

- (1) Prevention of further damage

- (2) Verification of facts and affected scope
- (3) Investigation of causes
- (4) Prevention of recurrence
- (5) Reporting to relevant authorities
- (6) Notification of individuals
- (7) Other measures required by law or customer protection

Reporting to the Personal Information Protection Commission and notifying affected individuals are undertaken in accordance with statutory thresholds, deadlines and procedures.

19. Matters Relating to Retained Personal Data

The Company publishes the following matters regarding retained personal data:

- (1) Name, address and representative of the personal information handling business
- (2) All purposes of use of retained personal data
- (3) Procedures for requests for notification of purposes of use or disclosure and related rights
- (4) Contact point for complaints concerning retained personal data
- (5) Summary of security management measures

The Company publishes details subject to change, including its address, representative and request contact point, under Company Information and Contact on its website.

20. Requests for Disclosure and Other Rights

Individuals or their duly authorized representatives may request the following using procedures designated by the Company:

- (1) Notification of purposes of use
- (2) Disclosure of retained personal data
- (3) Disclosure of records of third-party provision
- (4) Correction, addition or deletion
- (5) Suspension of use or erasure
- (6) Cessation of third-party provision

The Company verifies the identity and, where applicable, authority of the requester and responds in accordance with law.

The Company may decline a request in whole or part where permitted by law and, to the extent legally and operationally permissible, explains its reasons.

21. Procedures for Requests

Please submit the request form designated by the Company, identification documents and any other required materials to the prescribed contact point.

For requests by representatives, the Company may require identification of both the individual and representative and evidence of authority.

Disclosure methods, fees, response periods, delivery methods and other procedures are published on the Company website or in the guide to disclosure requests. Requests to the Company are free of charge as specified in that guide.

22. When the Company May Decline a Request

The Company may decline a request in whole or part in the following or other circumstances permitted by law:

- (1) Where there is a risk of harm to the life, body, property or other rights and interests of the individual or a third party
- (2) Where compliance would seriously hinder the proper conduct of the Company's business
- (3) Where compliance would violate a law
- (4) Where the identity or authority of the requester cannot be verified
- (5) Where the relevant retained personal data cannot be identified
- (6) Where the Company has no authority to disclose or otherwise process the data

23. Personal Information Complaints and Consultations

The Company accepts and endeavors to resolve appropriately and promptly complaints and inquiries about personal information.

Relevant departments investigate the circumstances and implement corrective measures and recurrence prevention when necessary.

24. Contact Details

Contact details for personal information, disclosure requests, complaints and inquiries are published on the Company website or by another means specified by the Company.

The contact information may include:

- (1) Name of inquiry desk
- (2) Address
- (3) Telephone number
- (4) Email address or inquiry form
- (5) Service hours
- (6) Other information needed to make an inquiry

Details that may change, including address, telephone number and service hours, are managed in the Company's website contact information rather than repeated in this Policy.

25. Accredited Personal Information Protection Organization

Where the Company is a covered business of an accredited personal information protection organization, it publishes the organization's name and contact details for complaints on its website or otherwise.

That organization is not the contact desk for questions concerning Company products or services.

26. Legal Compliance

The Company complies with the APPI, Payment Services Act, Act on Prevention of Transfer of Criminal Proceeds, other laws, guidelines and supervisory requirements.

27. Changes to this Policy

This Policy may be amended in response to legislative changes, changes in services or data processing and other circumstances.

Material amendments are published on the Company website or by other appropriate means.

28. Relationship to Internal Policies

Detailed management of personal and user information, safeguards, third-party and overseas disclosures, outsourcing, disclosure requests, breach responses and records is governed by Internal Policy 6-01, Information Assets, User Information and Personal Information Management Regulations, and Manual 6-02, Information Security and Personal Information Handling Procedures.

If this Policy conflicts with an internal policy, applicable law prevails and any inconsistency will promptly be corrected.

29. Repeal of Former Documents

The following former documents are repealed with effect from the commencement of this Policy:

(1) Former 20-1, Basic Policy on Personal Information Protection

(2) Former 20-2, Handling of Personal Information

The former 20-3, Provision of Personal Information to Third Parties, is incorporated into Schedule 1, Information on Provision of Personal Data to Third Parties in Foreign Countries.

Former versions are retained together with revision and consolidation records and comparison documents.

Schedule 1

Information on the Provision of Personal Data to Third Parties in Foreign Countries

To the extent necessary for international remittance services, the Company may transfer personal data to overseas remittance partners, receiving financial institutions, wallet operators and other such entities. The Company does not publish every contractual provision or internal audit record, but provides information required by law when seeking consent and responds to legally valid requests from individuals.

Principal destination countries/regions: Sri Lanka, Nepal and the Philippines. Recipient categories: remittance partners, receiving banks, wallet operators and similar entities. Purposes: executing international remittances, disbursement, transaction inquiries, cancellation and recall, AML and sanctions compliance, and preventing unauthorized use. Personally identifying information sent in ordinary remittance messages: the remitter's and beneficiary's names and cities. Amount, currency, reference number and other transaction data may also be processed. Images of identity documents, dates of birth and full addresses collected in Japan are not automatically included in standard remittance instructions. Additional disclosures in response to lawful inquiries are individually assessed. Under Articles 27 and 28 of the APPI, the Company obtains consent where legally required or implements other legally permitted measures and responds to requests for information in accordance with law.

Adoption and Revision History

Established: April 1, 2022

Consolidated revision: July 21, 2026