This Data and Privacy Protection Policy covers:

DATA AND PRIVACY PROTECTION POLICY

Transcash International Pty. Ltd. (ACN 147705324) trading as iPay, iSend, and iSend Global (the "Company"/ "Transcash") is a global cross-border payment operator holding an Australian Financial Services License granted by the Australian Securities and Investment Commission (ASIC), and registered with the Australian Transaction Reports and Analysis Centre (AUSTRAC). Transcash is fully committed to safeguarding the personal and sensitive information it collects and processes from its customers and stakeholders.

This Data and Privacy Protection Policy ("Policy") outlines our approach for the collection, use, protection, and management of personal data. It shall apply to all individuals and entities conducting business with us, as well as users who visit our website at www.ipayremit.com or www.isendremit.com.

We uphold individuals' right to privacy and ensure compliance with all applicable data protection laws, including the Privacy Act 1988 (Cth) (as amended), with particular attention to the 13 Australian Privacy Principles (APPs) outlined in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012. We also adhere to other relevant regulations in all jurisdictions where our products and services are offered.

In this Policy, references to "we", "our", or "us" refer to Transcash and any member of our corporate group responsible for delivering products or services and managing your personal data.

Collection of Personal Data

Personal data or personal information means any information about an identified individual, or an individual who is reasonably identifiable. It can include data you have shared, such as name, address, contact details, identification document, and others, as well as data we collect during your interaction with our services.

By submitting information through our portal to access our services, you confirm that the information provided is accurate, current, and that you are duly authorized to submit the personal details. You expressly acknowledge and consent to the use and verification of this information in accordance with the Company's policies and practices. You further confirm that you have read, understood, and agreed to the terms and conditions set out in this Policy.

For any concerns or queries, contact us at info@isend.com.sg or +61 476 058 772 (WhatsApp).

Information You Give Us

The information we hold about you is typically derived from data you provide directly, either during the registration process for our services or as needed thereafter. This encompasses:

a. *Contact details* (your name, email address, postal address, and phone number);

b. *Personal details* (date of birth, passport number, or other form of identification information, including national identification number, tax residency, tax reference number, proof of address, and proof of residency);

c. *Copies of identification documents* (passport, driving license, or other government-issued identification documents)

d. *Financial information* (bank account number, transaction history, and financial history);

e. *Your image in photo or video form* (including facial scan data extracted from your photo and video, known as "biometric data")

f. *The content of your communications with us* (emails, telephone call recordings, and chat messages);

g. *Source of funds* (we may request you provide information regarding the source of funds or wealth in specific circumstances).

The failure to provide any information that we tell you is needed to meet legal requirements might affect our ability to provide our services to you.

Information We Collect About You from Your Use of Our Services

Information such as transaction details that you carry out when using our services, details of the products you viewed or searched for, and page/app interaction information, may also be accessed by us.

Information We Receive from Other Sources

This includes:

a. *Information from financial institutions*: We may receive personal information from banks and financial institutions, for example, we may collect information about bank accounts that you choose to connect to your account with us.

b. *Information from connected persons*: If you are a "connected person" for our customer, then such customer may provide your personal data to us. For instance, if you're a payment beneficiary, data could include name, account details, email, and additional verification information if necessary for fulfilling our legal obligations or requested by the recipient bank.

c. *Information from fraud prevention agencies and government or private databases*: To verify your identification, we check the information you have provided to us against records held by government services such as the Document Verification Service (DVS) as well as private identity record databases or fraud prevention agencies to confirm your identity and combat fraud and other illegal activities.

d. *Information from publicly available sources:* We may collect information from publicly available sources, such as media stories, online registers or directories, and websites for enhanced due diligence checks and KYC purposes.

Ways We Use Your Information

We collect and use your personal data only for lawful and legitimate business purposes. Our handling of your data is guided by applicable privacy laws and is limited to what is necessary to deliver our services effectively, ensure regulatory compliance, and improve customer experience.

Legal Basis

We rely on one or more of the following legal bases when processing your personal information:

a. *Performance of Contract:* Where processing personal data is essential to enter into or fulfill our obligation under the agreement with you, such as executing a

transaction or providing a service you have requested.

b. *Compliance with Legal Obligations:* Where we are legally required to collect and process your information, such as verifying your identity and maintaining records under anti-money laundering (AML) and counter-terrorism financing (CTF) regulations, detecting, preventing, and prosecuting fraud and theft, as well as preventing illegitimate or prohibited use of our services or other illegal or wrongful activity.

c. *Legitimate Interests:* When data processing is necessary for our legitimate business needs, such as enhancing our services, maintaining security, managing risks, sharing promotional offers, or providing customer service, provided these interests do not override your rights and freedoms.

d. *Consent:* In certain circumstances, we will request your explicit consent prior to collecting or using your personal data. This applies in particular to the collection and use of biometric data, participation in optional services, receipt of marketing communications, and specific identity verification processes such as the Document Verification Service (DVS). You may withdraw your consent at any time. For further details, including how to manage or withdraw your consent, please refer to the Customer Rights and Requests section below.

Purposes for Using Your Personal Data

a. To verify your identity during onboarding to comply with relevant anti-money laundering and counter-terrorism financing regulations.

b. To process your transactions and provide services you have requested.

c. To manage your accounts, provide customer support, share relevant offers, improve the quality of our service, and identify any additional support you may need.

d. To prevent, detect, or protect against actual or suspected fraud, unauthorized transactions, claims, liability, and financial or other crimes, including conducting or cooperating with investigations of fraud or other illegal activity.

e. To meet our legal and regulatory obligations.

Third-Party Data Disclosure

Your data may be shared with the following third parties, only when necessary for business, legal, or regulatory purposes:

a. *Affiliated Companies:* Members of our corporate group, as well as service partners, to support service delivery, enhance operational efficiency, and assist with business functions.

b. *Financial Institutions:* Banks and other financial service providers involved in facilitating transactions. These parties operate independently and determine the purposes and means of processing your data.

c. *Advertising Partners:* Selected advertising networks that help deliver relevant marketing content, where permitted by law and/or with your consent.

d. *Regulatory and Legal Authorities:* Government bodies, regulatory agencies, law enforcement, and judicial or administrative courts, as required by law. This includes responding to subpoenas, warrants, court orders, or lawful requests, or where necessary to enforce our agreements or protect our rights, customers, employees, or others.

e. *Identity Verification Entities*: Government service providers such as DVS and private identity record databases to confirm your identity.

f. *Fraud Prevention Agencies:* Third parties engaged in the detection and prevention of fraud, unauthorized activity, and other financial crimes. This may involve cooperating with investigations and compliance obligations.

g. *Business Transfers*: In the event of a merger, acquisition, restructuring, or sale of assets, your data may be transferred to the relevant parties involved in the transaction, subject to confidentiality agreements and applicable data protection law.

Profiling and Automated Decision Making

To enhance your experience, ensure the security of our services, and personalize marketing communications, we may automatically collect data about your device, browsing pattern, location, and transaction history using various technologies, including cookies, local storage, pixels, web beacons, and flash cookies. You can opt out of receiving such communications at any time. For more information about the cookies and technologies we use, as well as their purposes, check our Cookies Policy.

In addition, we use automated systems to support the application and onboarding process, identity verification, and fraud detection. Based on risk analysis and verification results, these systems may decline an application, reject the transaction, or temporarily block an account login attempt. If such an automated decision affects you, we will notify you and provide the option to request further explanation and a manual review.

In cases where we, a fraud prevention agency or other third-party service provider, identify a risk of fraud or money laundering risk, we may be required to refuse access to our services or discontinue existing products and services provided to you in line with our legal obligations.

Data Retention

We maintain meticulous records of your personal data to fulfill the purposes for which it was collected. As a regulated entity, we are also legally required to retain certain personal and transactional data beyond the completion of a transaction or the closure of an account. These records may include, but are not limited to, transaction histories, client communications, service notifications, and documents provided by clients or their authorized representatives in relation to the services we offer.

All such records are retained for a period of seven (7) years in accordance with

applicable legal and regulatory requirements.

Data Security and Handling Guidelines

We implement strong technical and administrative measures to protect personal data from unauthorized access, loss, or misuse. Key measures include:

a. All personal data is encrypted as soon as it is entered into our systems to ensure it is protected from unauthorized access or misuse.
b. Access to data is limited to authorized employees on a need-to-know basis via Identity and Access Management (IDAM) controls.
c. Strong passwords, multi-factor authentication, and secure IT controls are used to protect data and prevent breaches.
d. Strict identity verification procedures are employed for customers requesting updates or corrections to their personal information.
e. Personal data is encrypted before transmission. Our IT team ensures that only approved and secure methods are used.
f. Personal data is never shared informally or with unauthorized individuals.
g. Personal data is not stored on local drives or personal devices.
h. Express consent is obtained from customers for DVS matches, the collection of biometric data, and identity verification.
i. Customers may restrict the use of their personal data for marketing purposes by contacting customer support. Personal data is never sold or disclosed to third parties, except when legally required.
j. Secure records are maintained to track who has accessed, modified, or deleted personal data, allowing for transparency and accountability.
k. Personal data is regularly reviewed to ensure that it is accurate and relevant. Data is retained only as long as required by business needs or legal obligations, and data that is no longer required is securely deleted.
l. Customers shall be clearly informed about how their data is collected, used, and shared. Where required, express consent will be obtained before using personal

data for specific purposes.

All Transcash employees are trained in data protection responsibilities and are expected to comply with our policies at all times. Although we cannot guarantee absolute immunity from sophisticated cyberattacks, we continually update our systems to reduce risks and enhance security.

Customer Rights and Requests

You have certain rights regarding the personal data we collect and process. Wherever possible, we will respond to your requests, which may include:

a. Request to access the personal data we hold about you
b. Request to correct or update inaccurate or incomplete data
c. Request to delete your personal data (subject to legal and identity verification requirements)
d. Request to opt out of optional services like direct marketing communications
e. Information on how your data is used and processed
f. Request to restrict or limit the processing of your personal data (including identity verification through DVS and overseas verification services)

You may submit any requests by contacting us at info@isend.com.sg. All requests will be managed securely and in compliance with applicable privacy protection laws.

Consent for Document Verification Service (DVS) Use

As part of our commitment to complying with regulatory requirements, we conduct identity verification of our customers using the Document Verification Service ("DVS"), a secure online system established under the Identity Verification Services Act 2023 (Cth) and governed by the Identity Verification Rules 2024, through authorized Gateway Service Providers. This might also extend to other parties involved in a particular transaction (for example, your recipient). In some cases, identity verification may be conducted by overseas personnel after obtaining

necessary approval from the relevant authority or through other identity verification services, both within Australia and internationally, as applicable.

The personal information obtained for identity verification through the DVS is used exclusively for that purpose and not for any unrelated or secondary purposes. It is handled and retained securely in accordance with this Policy and in compliance with all applicable laws and regulations, including the requirements outlined in the Document Verification Service Access Policy.

Our liability in relation to identity verification outcomes is limited to facilitating the verification process through authorized channels, including Gateway Service Providers and relevant government and private databases. While we take reasonable steps to ensure that the verification process is secure and complies with applicable laws and standards, we do not warrant or guarantee, to the extent permitted by law, the accuracy, completeness, or reliability of the information obtained from third-party data sources, including government agencies.

Nothing in this Policy excludes, restricts, or modifies any rights or consumer guarantees you may have under the Australian Consumer Law (ACL) or other applicable legislation. If you are a consumer for the purposes of the ACL and we fail to comply with a consumer guarantee in relation to the identity verification services we provide, our liability is limited, to the extent permitted by section 64A of the ACL, to either:

a. the resupply of the verification service; or
b. the payment of the cost of having the verification service resupplied,

unless it would not be fair or reasonable to limit our liability in this way.

Purpose

To comply with applicable legal and regulatory requirements, we must verify customer identities. This verification may involve matching your personal information against official records through the DVS and, where required, authorized verification services. The process is conducted securely and solely for

lawful verification purposes.

Scope of Consent

By engaging with our services, you acknowledge and provide your informed consent to the following, with such consent being specific, current, and given by an individual with the legal capacity to do so:

a. You represent and warrant that the information provided is accurate, complete, current, and valid. You further confirm that you are duly authorized to provide the personal information submitted and expressly acknowledge and consent to its use for the purposes of identity verification through the DVS, including the use of other verification services where applicable.
b. We are authorized to verify your identity using the DVS through an authorized Gateway Service Provider. This verification will be conducted by our authorized personnel, including those based overseas, or through other duly authorized verification services within Australia and overseas.
c. The following details that you have provided will be matched against official records for verification purposes:
    i. Full name
    ii. Date of Birth
    iii. Passport/Driver's License/National ID details
    iv. Any other identity documents required for verification
d. The verification process will be conducted securely, and your information will only be used for lawful identity verification.

For more detailed information on identity verification via the DVS, you may refer to our DVS Data Use and Disclosure Statement.

Withdrawal of Consent and Complaint Handling Mechanism

You may withdraw your consent regarding the use of DVS at any time by providing written notice to info@isend.com.sg. Please note that withdrawing your consent

may impact our ability to deliver certain services to you.

If you have any questions regarding access to your personal information, or if you wish to request corrections or lodge a complaint about its handling, you may contact us using the details provided. If your concerns remain unresolved, you may escalate the matter to the Attorney-General's Department of Australia, which serves as the DVS Hub Manager.

Responsibilities and Oversight

All of our employees receive training and are expected to follow all related protocols to comply with their data protection responsibilities. The Compliance Head or a staff member of equivalent seniority is designated as the Data Protection Officer ("DPO") to ensure compliance with the relevant laws. When a data breach occurs, the DPO will forthwith report to Senior Management and will be responsible for initiating appropriate response and remediation measures to the data breach.

You can contact our DPO at info@isend.com.sg for any concerns regarding data and privacy protection. If you feel that we have not sufficiently addressed your questions or concerns, or if you believe that your data protection or privacy rights have been compromised, you have the right to file a complaint with any relevant supervisory authority including the Australian Financial Complaints Authority (AFCA) or public body responsible for enforcing privacy laws.

Policy Reviews and Updates

This Policy is subject to periodic review and amendments as deemed necessary by our Senior Management to ensure ongoing relevance and legal compliance. In the event of material changes, we will notify customers appropriately.

The most current version of this Policy will be publicly available on our website.

Acknowledgement and Consent

☐ By submitting information through our portal to access our services, you confirm that the information provided is accurate, current, and that you are duly authorized to submit the personal details. You expressly acknowledge and consent to their use and verification through DVS and other verification services in accordance with the Company's policies and practices.

☐ You also acknowledge that you have read, understood, and agreed to the terms and conditions of this Policy.

For any concerns or queries, contact us at info@isend.com.sg, or +61 476 058 772 (WhatsApp).

By submitting information through our portal to access our services, you confirm that the information provided is accurate, current, and that you are duly authorized to submit the personal details. You expressly acknowledge and consent to the use and verification of this information in accordance with the Company's policies and practices. You further confirm that you have read, understood, and agreed to the terms and conditions set out in this Policy.

For any concerns or queries, contact us at info@isend.com.sg or +61 476 058 772 (WhatsApp).