

This Data and Privacy Protection Policy covers:

- ❖ Collection of Personal Data
 - Information You Give Us
 - Information We Collect About You from Your Use of Our Services
 - Information We Receive from Other Sources
- ❖ Ways We Use Your Information
 - Legal Basis
 - Purposes for Using Your Personal Data
- ❖ Third-Party Data Disclosure
- ❖ Profiling and Automated Decision Making
- ❖ Data Retention
- ❖ Data Security and Handling Guidelines
- ❖ Customer Rights and Requests
- ❖ Responsibilities and Oversight
- ❖ Policy Reviews and Updates
- ❖ Acknowledgement and Consent

DATA AND PRIVACY PROTECTION POLICY

Isend Pte. Ltd. trading as iSend (the “Company”/ “iSend”) is a global cross-border payment operator holding a Major Payment Institution license granted by the Monetary Authority of Singapore (MAS). iSend 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 and users who visit our website at www.isendremit.com.

We uphold individuals’ right to privacy and ensure compliance with all applicable data protection laws, including Singapore’s Personal Data Protection Act, the EU General Data Protection Regulation, the UK Data Protection Act, as well as other relevant regulations in all jurisdictions where our products and services are offered.

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

Collection of Personal Data

Personal data refers to data about an individual who can be identified from the data, or from the data and other information to which the organization has or is likely to have access. 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.

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:

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 +65 8386 1948 (WhatsApp).

- 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 to 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

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.

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:* In order to verify your identification, we check the information you have provided to us with government or private identity record databases, or fraud prevention agencies, to confirm your identity and to combat fraud.
- 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

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.

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 specific situations, we will seek your explicit consent before collecting or using your personal data. This includes, in particular, the collection and use of biometric data, as well as participation in optional services or receipt of marketing communications. 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 and at other times, such as when registering a new device or updating personal information, to comply with applicable 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.

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.

- 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. *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.
- f. *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

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.

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 five (5) 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

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 +65 8386 1948 (WhatsApp).

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. Consent is obtained from customers for identity verification, as well as before the collection of biometric data.
- 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 iSend 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. Access to 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 verification requirements)
- d. Request to opt out of receiving direct marketing communications
- e. Information on how your data is used and processed

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 +65 8386 1948 (WhatsApp).

f. Request to restrict or limit the processing of your personal data

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.

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 Monetary Authority of Singapore (MAS) 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 avail our services, you confirm that the information provided is accurate, current, and that you are duly authorized to provide the personal details submitted and consent to

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 +65 8386 1948 (WhatsApp).

their verification 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 [+65 8386 1948](tel:+6583861948) ([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 +65 8386 1948 (WhatsApp).