



## GLOBAL PRIVACY POLICY

### Introduction

Our group company known as **Paysend** ("Paysend," "we," "our," or "us") values your privacy and is committed to protecting your personal data. The company with whom you contract when you become our customer ("Data Controller") is the company responsible for looking after the personal information that you provide to us. You can find out more about each Data Controller in the section further down.

**This Global Privacy Policy is the group-wide baseline that applies to all Paysend entities and their customers worldwide. For users in the United Kingdom, the European Economic Area (EEA), Canada, and the United States, entity-specific Privacy Notices have been published at [paysend.com/rules](https://paysend.com/rules) that provide supplementary detail required by local law. Those notices complement this Policy and should be read alongside it.**

This Global Privacy Policy explains how we collect, use, store, and share your personal information, including biometric data, in compliance with applicable privacy laws — including the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy legislation, the Gramm-Leach-Bliley Act (GLBA) in the United States, and other applicable data protection legislation. For details specific to biometric data collection in your jurisdiction, please refer to the country-specific Facial Scan Notice at [paysend.com/rules](https://paysend.com/rules).

**This Global Privacy Policy does not apply to users in Australia, El Salvador, Guatemala, Honduras, Jamaica. Please refer to the appropriate local privacy policy at [paysend.com/rules](https://paysend.com/rules).**

---

### 1. What Personal Information Do We Collect?

Depending on our relationship and interactions with you, the categories of Personal Information we collect may include:

- **Personal contact information:** Name, email address, home address, phone number, date of birth.
- **ID information:** Government-issued identification, document type, issuing country, ID number, expiry date, MRZ, barcodes, security features; and proof of address (PoA) document data.
- **Biometric data:** Liveness checks and face-match images (selfie and short liveness capture); facial biometric templates; voice checks and audio testimonials; and any mathematical representation or match score derived from such data, as further described in our Facial Scan Notice at [paysend.com/rules](https://paysend.com/rules).

- **Financial, reference, and credit information:** Banking details (cardholder name, expiry date, first 6 and last 4 digits of the card number), payment details, transaction history, creditworthiness verification, card numbers, bank statements, employment information (e.g., employer name and employment status), government-issued ID numbers, and pictures of your ID, utility bills, and other documents.
- **Consumer credit report information.**
- **Transaction information:** information about when and where your transactions occur, the names of the transacting parties, a description of the transactions, the payment or transfer amounts, billing and shipping information, and the devices and payment methods used to complete the transactions.
- **Device and usage data:** information about the geographic location and specifics of your device, including your hardware model, operating system and version, unique device identifier, mobile network information, information about the device's interaction with our Services, and information about other software running on the device, IP address, domain name, browser type, access time, and language.
- **Marketing communications and interaction information:** the content and metadata (meaning records) associated with these communications, and other information you provide when you participate in contests or promotions offered by us or our partners or respond to our surveys; your email address as well as other information. You can unsubscribe at any time by clicking the "unsubscribe" link included at the bottom of each email.
- **Cookies:** Our website uses a technology called "cookies". Some cookies may be used to track your online behaviour across services, which may be used for profiling. For more information on our use of cookies, including to manage your cookie settings, please see our Cookies Policy.
- **Analytics data:** We may use a third party such as Google Analytics to help us gather and analyse information about the areas visited on the website (such as the pages most read, time spent, search terms, and other engagement data) in order to evaluate and improve the user experience and the website. For more information about Google Analytics or to prevent the storage and processing of this data (including your IP address) by Google, you can download and install the browser plug-in available at the following link: <https://tools.google.com/dlpage/gaoptout?hl=en>. You can also obtain additional information on Google Analytics data privacy and security at the following links: <https://policies.google.com/technologies/partner-sites>, <https://support.google.com/analytics/topic/2919631>
- **Tax information:** Country or countries of tax residence, tax identification number(s) or equivalent issued by a tax authority, information provided in tax self-certification forms,

and other information used to determine your tax residency status under international tax transparency regimes such as the Common Reporting Standard (CRS).

## 2. How do we collect your personal information?

We may collect Personal Information about you from various sources, depending on our relationship and interaction with you. These sources may include;

- directly from you (online through our Services and forms, including when you register for a Paysend account or communicate with us), or
- indirectly from third parties, who give us your personal information to provide our services, or
- from our business clients with whom you have a relationship, and who may pass on your personal information so that we can help them deliver their services to you, or
- from financial institutions, or
- third-party identity verification services when we're performing identity verification, which includes the processing of biometric data while capturing your face and processing of the biometric identifies, taking facial scan image(s) of you (which is part of our onboarding process), during your account verification process (when you call us or make a transaction request for instance), or
- your computer or devices when you interact with our platforms, websites, and applications or through other automatic technologies.
- from publicly available sources where permitted by law, which may include government and regulatory databases, commercial and corporate registries, and other sources that are lawfully and publicly accessible.

Where we obtain your data from third parties (e.g., fraud prevention agencies, marketing partners), we ensure they have collected it lawfully and provide notice where required.

## 3. Why We Collect Personal Information and How We Use It?

We collect personal data to:

Purpose for Collecting and Sharing	Categories of Personal Information	Legal Basis for Processing
<ul style="list-style-type: none"> <li>• Provide and improve our services: create, administer, and enable your use of your Paysend account our Services.</li> </ul>	<ul style="list-style-type: none"> <li>• Personal contact information</li> <li>• Financial, reference, and credit information</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Contractual Necessity: When processing is required to fulfil contractual obligations, such as providing payment and transfer services.</b></li> </ul>

<ul style="list-style-type: none"> <li>• Verify your identity for Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance</li> <li>• Prevent fraud and unauthorized access.</li> </ul>	<ul style="list-style-type: none"> <li>• ID information and biometric data</li> <li>• Personal contact information</li> <li>• Financial, reference, and credit information</li> <li>• Device and usage data behaviour, and location</li> <li>• Transaction history</li> </ul>	<ul style="list-style-type: none"> <li>• Legal Obligation: Compliance with AML/CFT regulations applicable in each jurisdiction (including PCMLTFA in Canada and UK/EU AML Directives in the UK and EEA); Substantial Public Interest (under UK GDPR and EU GDPR Article 9, where applicable to biometric and special-category data).</li> <li>• Consent: Where explicit consent is required for biometric data processing under applicable local law. Legitimate Interest: Where processing is necessary for fraud prevention and security, balanced against your rights and freedoms.</li> </ul>
<ul style="list-style-type: none"> <li>• Verify your identity for Know Your Customer (KYC) and the identity of your recipients or as required for any other purpose related to providing our services</li> </ul>	<ul style="list-style-type: none"> <li>• Consumer credit report information</li> </ul>	<ul style="list-style-type: none"> <li>• Contractual Necessity</li> </ul>
<ul style="list-style-type: none"> <li>• Comply with international tax reporting and transparency obligations, including reporting account information and, where relevant, controlling persons of entity customers to appropriate tax authorities under automatic exchange of information (AEOI) arrangements such as the Common Reporting Standard (CRS).</li> </ul>	<ul style="list-style-type: none"> <li>• Tax information; Personal contact information; Financial, reference, and credit information; Transaction information.</li> </ul>	<ul style="list-style-type: none"> <li>• Legal Obligation: Compliance with international tax reporting laws and AEOI frameworks applicable in each jurisdiction.</li> </ul>
<ul style="list-style-type: none"> <li>• Provide and improve our services: create, administer, and enable your use of your Paysend account our Services</li> <li>• Anti-Money Laundering (AML) compliance under the Proceeds of Crime (Money Laundering)</li> </ul>	<ul style="list-style-type: none"> <li>• Transaction information</li> </ul>	<ul style="list-style-type: none"> <li>• Contractual Necessity</li> <li>• Legal Obligation</li> </ul>

<ul style="list-style-type: none"> <li>• For anti-fraud and malware-prevention purposes</li> <li>• To improve, personalize, facilitate, and track and analyse trends in your use of our Services (for example, when you sign up for a Paysend account, we may associate certain information with your new account, such as information about prior transactions you made using our Services)</li> </ul>	<ul style="list-style-type: none"> <li>• Device and usage data behaviour, and location</li> <li>• Transaction history</li> </ul>	<ul style="list-style-type: none"> <li>• Legitimate Interest</li> </ul>
<ul style="list-style-type: none"> <li>• To tailor marketing content and marketing communications and/ or to participate in contests or promotions offered by us or our partners, or respond to our surveys</li> </ul>	<ul style="list-style-type: none"> <li>• Marketing communications and interaction information</li> <li>• Device and usage data behaviour, and location</li> <li>• Transaction history</li> </ul>	<ul style="list-style-type: none"> <li>• Legitimate Interest</li> </ul>
<ul style="list-style-type: none"> <li>• To recognize the user's computer or device when they return, to evaluate and improve the user experience and the website</li> <li>• To customize and enhance the design, content, and functionality of our Mobile App and website</li> </ul>	<ul style="list-style-type: none"> <li>• Cookies and Analytics data</li> </ul>	<ul style="list-style-type: none"> <li>• Legitimate Interest</li> <li>• Consent</li> </ul>

---

#### 4. Information Security and Data Retention

We use physical, technical, organisational, and administrative safeguards to help protect your Personal Information from unauthorized access or loss. For example, we use encryption and other tools to protect sensitive information. We retain your Personal Information as needed for the purposes listed above and as permitted by law.

Different categories of personal information may have different retention periods. Transaction and financial records are retained for up to 10 years after your Paysend account is closed, or the maximum period required by applicable law or legal process, whichever is longer — based on

regulatory and contractual obligations, including financial compliance, fraud prevention, and dispute resolution. Biometric records (including raw images, facial templates, and match scores) are retained only for as long as necessary for the identity verification, fraud-prevention, or security-review purpose for which they were collected, and are destroyed once that purpose has been met or no longer exists.

---

## 5. Categories of Third Parties and Our Disclosure of Personal Information

We may disclose your Personal Information to:

- **Paysend Affiliates** within our corporate group to ensure seamless service integration and compliance with international security measures. Where personal data is transferred to affiliates outside Canada, Paysend CA Limited remains accountable for its protection and ensures that comparable privacy safeguards are applied, in accordance with PIPEDA and applicable provincial privacy laws.
- **Third-party providers** who process personal data strictly under contract. Their categories;
  - a. identification and verification services, which verify your identity
  - b. data management and storage services, where we store your information and backups in the same
  - c. systems applications that we use to manage and store data internally in a structured way
  - d. marketing partners, who assist us in providing you with our marketing content
  - e. financial institutions, who help us process your payments and deliver the same to your recipients
  - f. debt collection agencies, who we may need to instruct in the event of payment deficits
  - g. analytics and search engine providers that assist us in the improvement and optimisation of our site
- **Fraud/Crime Prevention Agencies, including regulatory authorities.**
- **Other Users of the Services:** facilitating your usage of our services, we share with other users that have you saved in their phone's contact list information that you're also using our services (if you opt-in to share this information with such users).
- **Law enforcement agencies**, regulators, or courts, where legally required or as permitted by other laws.
- **Tax and other competent authorities:** where required under automatic exchange of information (AEOI) regimes such as the Common Reporting Standard (CRS), we may share information about you, your accounts, and your transactions with tax authorities or other competent authorities in countries where we are obligated to do so.

## 6. International Transfers

Paysend and its global affiliates and service providers may process and transfer your Personal Information across international borders, including to countries that may not offer the same level of data protection as your home jurisdiction. Regardless of where your data is stored or accessed, we ensure that it is handled securely and in accordance with this Privacy Policy and applicable international data protection standards. Where required by law, we implement appropriate safeguards — such as the European Commission’s Standard Contractual Clauses (SCCs) and, where applicable, the UK Addendum to the SCCs — to ensure your data remains protected during cross-border transfers. For transfers of personal information outside Canada, Paysend CA Limited conducts a privacy impact assessment, reviews the laws and safeguards in the receiving country, and implements written contractual protections to ensure adequate protection.

---

## 7. Your Rights and Choices

Depending on your country’s laws, you may have rights such as:

- **Right to be informed.** You have the right to know how we collect, use, share, and protect your personal data. This includes what data we collect, why we need it, how long we keep it, and who we may share it with.
- **Right to access** your personal data/**to obtain confirmation** as to whether or not your personal data are being processed;
- **Right to rectification, to correct inaccuracies** in your data, or, in other words, to correct the wrong information or complete it;
- **Right to erasure or “right to be forgotten”.** Please note that this right is not absolute and applies only if (i) your personal data is no longer necessary in relation to the purposes for which was collected or otherwise processed, (ii) you object to the processing, and there are no overriding legitimate grounds for the processing of Paysend; (iii) the Personal data have been unlawfully processed.
- **Right to restrict personal data processing:** where (i) the accuracy of the personal data is contested (during the period when Paysend is able to verify its accuracy); (ii) the processing is unlawful, and you object to the erasure of the Personal data and request to restrict their use instead; (iii) Paysend no longer needs the Personal data for the purposes of the processing, but they are required by you to establish, exercise or defend legal claims; (iv) you have objected to processing pending the verification whether Paysend’s legitimate grounds override those of yours;

- **Right to be informed** as to rectification or erasure of personal data or restriction of their processing;
- **Right to data portability**, or, in other words, receive your information in a structured machine-readable format (for instance, in a pdf or excel document) (data portability in tech terms), which will enable you to, for instance, migrate your personal information elsewhere.
- **Right to avoid automated decision-making including profiling**, unless (i) such decision is necessary for entering into, or performance of, a contract between us; (ii) such decision is authorised by the law to which Paysend is subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests or (iii) such decision is based on your explicit consent; in this case you have a right to request human intervention, express your point of view, and contest decisions made solely by automated means;
- **Right to object to personal data processing if the processing is justified by the ‘public interest’ or ‘legitimate interest’ legal grounds as set out in points (e) and (f) of Article 6(1) of the GDPR, including profiling based on those provisions;**
- **Right to object to marketing-related profiling** and to withdraw your consent to receive marketing communications at any time. You can do this by clicking the “unsubscribe” link in our emails or by contacting us at [dataprotection@paysend.com](mailto:dataprotection@paysend.com);
- To opt-out of Cookies; to manage your cookie settings, please see our Cookies Policy.
- **Right to right to lodge a complaint with a supervisory authority** if your data is mishandled.

To exercise your rights, contact [dataprotection@paysend.com](mailto:dataprotection@paysend.com). Alternatively, you may use the technical tools and features of your Paysend Account, which will connect you with our customer services team through our chat function.

The specific rights available to you depend on your country of residence and applicable local law. Users in the United Kingdom and EEA, Canada, and the United States should also refer to their entity-specific Privacy Notice for the full set of rights applicable to them under local law.

## **8. Automated Decision-Making and Profiling**

We use automated systems and decision-making processes—including profiling techniques—to help verify your identity, prevent fraud, comply with anti-money laundering laws, and manage risk associated with financial transactions. These processes may analyze your personal and transactional data to identify patterns that signal potential risk.

Where significant decisions are made solely or partly by automated means, we ensure appropriate safeguards to protect your rights. These include: (i) providing you with meaningful information about the logic involved and the potential consequences of the decision; (ii) enabling you to request access to the personal data used; (iii) allowing you to correct any inaccuracies; (iv) enabling you to

make representations and challenge the decision; and (v) providing you the right to obtain human intervention in the decision-making process.

We use profiling for marketing purposes. This involves automatically analysing your personal data (such as location, transaction history, and service usage) to determine which products or offers may interest you. These decisions do not have legal or similarly significant effects, but you have the right to object to profiling for direct marketing at any time.

## 9. Children's Privacy

Paysend does not knowingly collect personal information from individuals who are under the minimum age required to use our services in their country of residence. If we become aware that we have inadvertently collected personal information from a minor without proper parental or guardian consent, we will take immediate steps to delete the data under applicable laws and regulations.

## 10. Data Controllers

Your data controller depends on your country of residence and the services you use. You can find a list of our local entities at the table below.

For users in the United Kingdom and European Economic Area (EEA), Paysend Plc and Paysend EU DAC act as joint controllers under Article 26 of the UK GDPR and EU GDPR, jointly determining the purposes and means of processing personal data in those jurisdictions. Paysend Plc serves as the lead controller and is responsible for responding to data subject requests, managing privacy enquiries, and coordinating with supervisory authorities, including the Information Commissioner's Office (ICO) and the Data Protection Commission (DPC). The essence of the joint controller arrangement is available upon request.

Country Region	Data Controller	Supervisory Authority
United Kingdom and other territories not territory (except Australia, Canada, the EEA, El Salvador, Guatemala, Honduras, Jamaica, and the United States)	Paysend Plc  Address: 1st Floor, 20 Garrick Street, London WC2E 9BT, United Kingdom	Information Commissioner's Office (ICO) <a href="http://www.ico.org.uk">www.ico.org.uk</a>
EEA	Paysend EU DAC  Address: 6th Floor South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland	Data Protection Commission (DPC) <a href="http://www.dataprotection.ie">www.dataprotection.ie</a>

Canada	<p>Paysend CA Limited</p> <p>Address: 2800 Skymark Ave, Suite 300, Mississauga, ON L4W 5A6, Canada</p>	<p>Office of the Privacy Commissioner of Canada</p> <p><a href="http://www.priv.gc.ca">www.priv.gc.ca</a></p>
US	<p>Paysend US LLC</p> <p>Address: PAYSEND, 801 Brickell Avenue, 8th Floor, Miami, FL 33131</p>	<p>Consumer Financial Protection Bureau (CFPB)</p> <p><a href="https://www.consumerfinance.gov/">https://www.consumerfinance.gov/</a></p>

---

### 11. Contact Information

For questions about this Global Privacy Policy or to exercise your rights, contact by e-mail:

Paysend Group Data Protection Officer

Email: [dataprotection@paysend.com](mailto:dataprotection@paysend.com)

---

This notice was last updated on [June 2026]. We may update it periodically, and we encourage you to review it regularly. We will notify you of any material changes to this Privacy Policy by email or within the app/website interface.