MoneyGram Global Privacy Notice

Last Updated October 2026

MONEYGRAM GLOBAL PRIVACY NOTICE

Key Points

This is a summary of the most important points about how MoneyGram handles your personal data. For full details, please see the relevant sections of this Privacy Notice.

1. **Who is responsible for your data:** MoneyGram Payment Systems Inc., and its relevant group entities act as data controller(s) in respect of your personal data. To find out how to contact us, see the "*How to contact us?*" section of this Notice.
2. **Why and on what basis we use your data:** We use your personal data for the following purposes and on the following legal bases:
    - *Contract performance* — to provide money-transfer and financial services, complete your transactions, authenticate you, respond to your queries, and give you access to our digital platforms.
    - *Legal obligation* — to comply with AML, sanctions, fraud-prevention, tax, accounting, and other regulatory requirements, and to respond to lawful requests from courts, regulators, and law enforcement.
    - *Legitimate interests* — to improve and secure our services, personalise your experience, enforce our terms, protect our business and customers, and for general business management and internal administration.
    - *Consent* — to send marketing communications, display interest-based advertising, and for other purposes where we have asked for and obtained your consent. You may withdraw consent at any time.

1. **Sensitive data:** Where required to verify your identity, we may process identity document data and, where applicable, biometric data. See Section *"What categories of your personal data do we collect or process?"* for further detail.
2. **Who we share your data with:** Your personal data may be shared with MoneyGram group companies, agents, payout partners, banks, payment processors, identity-verification and fraud-prevention providers, technology providers, regulators, and law enforcement. For more details on data sharing, see Section *"How do we share your personal data?"*
3. **International transfers:** As a global business, MoneyGram may transfer your personal data internationally, including to the United States. Where required by law, appropriate safeguards are applied. See Section *"How do we transfer your personal data to third countries?"* for details.
4. **How long we keep your data:** We retain your personal data only for as long as necessary for the purposes described in this Notice, or as required by applicable law. See Section *"How long do we retain your personal data?"* for more details.
5. **Automated decision-making:** Where we carry out automated decision-making or profiling that has a significant effect on you, we will provide further information at the point of collection. See Section "***Do we make automated decisions or use profiling?***" for details.

MoneyGram Global Privacy Notice

Last Updated October 2026

6. **Your rights:** Depending on your location, you may have the right to access, correct, delete, restrict, object to, or port your personal data, withdraw consent, opt out of marketing or certain targeted advertising, and lodge a complaint with a data protection authority.
7. **How to exercise your rights:** To submit a request or complaint, or to obtain more information — including about the balancing tests we carry out for legitimate interest processing — please use the contact details in the "***How to contact us?***" section of this Notice.

In this Global Privacy Notice (the "**Notice**"), "MoneyGram," "we," "us" and "our" mean the MoneyGram company that determines how and why your personal data is used in connection with the relevant Service or interaction. References to the "MoneyGram group" mean MoneyGram and its affiliated companies. We respect your privacy and are committed to handling your personal data responsibly and in accordance with applicable laws. This Notice is intended to explain our practices in a clear, accessible and transparent way, while also providing the legal information required in the countries and regions where we operate.

This Notice applies to "you" when you interact with us as our customer, prospective customer, transaction sender, transaction receiver, website or app user, loyalty-program member, marketing recipient, social-media user, or prospective agent or business partner. It applies when you use our money transfers, other financial services worldwide, wallet services available through our mobile app, or any other services we provide, whether through digital platforms, mobile applications, websites, retail locations, agents or other partners ("Services"). Where we process personal data about a transaction receiver, beneficiary, wallet user, or another person identified in connection with a transaction or Service, this Notice also explains how we use that person's personal data, even if that person does not interact with us directly.

This Notice explains: what information we collect about you, why we collect it, what we do with it, and what your rights are related to the use of your data. Below you will find information on:

1. Who is the data controller?
2. Who is the data protection officer?
3. What categories of your personal data do we collect or process?
4. Why do we collect, use, and store your personal data?
5. Who do we share your personal data with?
6. How do we transfer your personal data to third countries?
7. How long do we retain your personal data?
8. What are our information security standards?
9. What are your choices and rights?

MoneyGram Global Privacy Notice

Last Updated October 2026

10. How to submit a complaint to a supervisory authority?
11. Do we make automated decisions or use profiling?
12. How do we notify you about changes to this Notice?
13. How to contact us?
14. Local supplements

MoneyGram's processing of personal data is in all cases subject to the requirements of applicable local law and, to the extent this Notice conflicts with laws in your country, local law prevails. We may include local supplements in this Notice that cover specific local issues.

We may also provide you with additional information when we collect personal data, where required by law or where it is useful to provide relevant and timely information for example through in-app notices, cookie banners, transaction forms, agent forms, consent screens or other just-in-time notices.

We do not provide Services directly to children and our Services are not intended for children. We do not knowingly collect personal data directly from children, except where permitted or required by applicable law. In limited cases, we may process personal data relating to a child where necessary and permitted by applicable law, such as where a child is identified as a transaction receiver or where the processing is required for legal, regulatory, compliance, and fraud prevention purposes. We do not knowingly sell or share personal data of children where prohibited by applicable law.

The MoneyGram website, app and other digital platforms may contain links to third-party websites, apps, plug-ins or services. When clicking on a third-party advertising banner or other links on the MoneyGram website, you may be redirected to that third-party website. We are not responsible for the privacy practices of those third-party websites or services, and we encourage you to review their privacy notices before providing personal data to them.

MoneyGram Global Privacy Notice

Last Updated October 2026

1. Who is the data controller?

MoneyGram conducts its business primarily through the wholly-owned subsidiary MoneyGram Payment Systems Inc., a U.S. entity located at 1550 Utica Avenue South, Suite #100, Minneapolis, MN 55416 ("**MPSI**"). MPSI is generally the controller for processing related to the global operation of the Services and certain MoneyGram marketing activities, unless another MoneyGram company is identified as controller in the controller list, in the Local Supplement section of this Notice, or in a product-specific notice. The data controller for the non-custodial wallet is MoneyGram Software Services, Inc., with its registered address at 1550 Utica Ave S, Ste 100, Minneapolis, MN 55416. However, depending on your location and the way you interact with MoneyGram, a different MoneyGram company may be the data controller. For example, if you use Services in the European Economic Area ("**EEA**"), you will be interacting with MoneyGram International SA, a Belgian entity with its registered address at Rue Joseph Stevens 7, BE-1000 Brussels ("**MIS**"), which is the data controller for the relevant EEA Services, unless a local supplement or product-specific notice states otherwise. Where we act as a processor or service provider on behalf of another organisation, that organisation's privacy notice may also apply.

Please click here for a list of the companies that are data controllers, depending on your location and the way you interact with them.

2. Who is the data protection officer?

Some MoneyGram companies have appointed a data protection officer or equivalent ("**DPO**") to oversee the processing of personal data. Where a MoneyGram company is required by applicable law to appoint a DPO or local privacy contact, we provide the relevant contact details in the controller list or applicable local supplement. Click here to check which company has appointed a DPO and how to contact the DPO.

3. What categories of your personal data do we collect or process?

The categories of personal data we collect or process will vary based on your relationship or interaction with us. This may include the following:

- **Identity and contact information**, such as your name, residential and/or business address, e-mail address, telephone number, date of birth, gender, place of birth, nationality, citizenship, occupation, employer, source of funds, relationship to the transaction receiver, images, marital status, country of citizenship, and identification numbers (e.g., national identification number(s) and /or national ID details);
- **Identity-verification and compliance information**, such as copies or details of government-issued identification documents, proof of address, biometric data or biometric identifiers where used and permitted by law, sanctions, politically exposed person and adverse-media screening results, fraud-prevention indicators, risk scores, transaction-monitoring alerts, and information required for anti-money laundering, counter-terrorist financing, sanctions, consumer-protection, tax, accounting or other regulatory purposes;
- **Transaction and financial details**, such as money transfer data relating to the sender and the receiver, bill paying details, transaction reference numbers, payment method, bank, card, wallet or account details, payout method, currency, amount, fees, exchange rate, transaction status, transaction history, recipient details, wallet data where relevant to a Service, and other bank, payment and credit information where relevant to the Service;

- **Business-related and account information** that helps us provide Services to you, such as membership in our loyalty programs, how you use our Services, employer information, communication language preferences customer segment, rewards activity, or your marketing choices;
- **Technological information and online activity information**, such as IP address, browser, device information, including device identifiers and device's advertising ID, mobile application usage data, information collected through cookies, pixel tags, browser analysis tools, server logs, web beacons, SDK and other similar technologies (collectively, cookies), your current location from your mobile device. For details on how we use cookies, please see our Cookie Notice; and
- **CCTV and security information**, such as closed-circuit television footage and other security-related information collected at our premises, agent locations or other relevant locations, where used for security, safety, fraud-prevention, incident-management or compliance purposes and permitted by applicable law; and
- **Agent, partner or business-contact information**, where you apply to become our agent or otherwise interact with us in a business capacity, such as business contact details, ownership, management, due diligence, licensing, compliance, financial and contractual information.

We collect personal data directly from you, for example, when you contact our call center, complete online forms, register for our loyalty programs, apply to become an agent, or use the Services. In some situations, we also collect personal data about you from other people or organizations such as: money transfer senders, receivers or other transaction participants, our third-party vendors, identity-verification providers, fraud-prevention agencies, sanctions and politically exposed person screening providers, payment processors, banks, card schemes, wallet providers, payout partners, credit reference or background-check providers where permitted by law, public record sources (federal, state or local government sources), MoneyGram affiliates and subsidiaries, social media platforms, MoneyGram partners or agents, law enforcement bodies, regulators or other competent authorities, depending on our relationship with them.

Some of the information listed above may be considered sensitive personal data, special category data or sensitive personal information under applicable law. Where this is the case, we process it only where we have an appropriate legal basis and, where required, an additional legal condition or your consent.

4. Why do we collect, use and store your personal data?

We must have a lawful basis for processing your data. We explain this in the table and subsequent section on marketing communications below. We also explain the purposes for which we use your data. The lawful basis may differ depending on your country, the Service used and the type of personal data involved. Local supplements may provide additional or different information where required by local law. Where we rely on legitimate interests, we consider and balance our interests against your rights, freedoms and reasonable expectations.

Lawful ground	Processing purposes
Contractual performance - we have obligations under our contract with you. To fulfil these obligations, we have to use your data.	• to identify your device and authenticate you, • to perform a Service, including to complete your transactions (when you are a transfer sender) or other

	requests made by you, and to contact you in connection with the performance of a contract and the provision of the Service, in particular to send you transactional and other administrative messages e.g., on updates to Services (via email, SMS or push notification, depending on your preferences), • to respond to and process your queries, and • to provide you with our digital platforms.
Compliance with a legal obligation - as an organization, we have obligations to comply with legal, regulatory and other requirements under applicable laws. In certain cases, we will have to use your data to meet these obligations.	• to monitor and prevent fraud, money laundering, or other prohibited or illegal activities, • to screen personal data about you obtained from third parties — such as transaction counterparties, payout partners, or public databases — against sanctions lists, watchlists, and other legally required checks, • to comply with our legal obligations and regulatory requirements (e.g., tax, accounting, data protection), • to respond to court orders, subpoenas, warrants, regulatory requests, law-enforcement requests or other valid legal processes where we are required by law to do so, respond to requests from public and governmental authorities and to cooperate with law enforcement, and • for other legal reasons, as applicable.
Legitimate business purposes (legitimate interest) - we can process your data where this is necessary for our legitimate interests or the legitimate interests of a third party, provided that those interests are not overridden by your interests, rights and freedoms. We explain in the right-hand column what interests we, or others, are trying to achieve when we process your data. Where we process personal data on the basis of legitimate interest, then – as required by data protection law – we have carried out a balancing test to document our interests, to consider what impact the processing will have on individuals, and to	• to receive personal data about you as a transaction recipient from the sender of a transfer, and to use that data to complete the transaction and make funds available to you, • to combine data we hold about you with data received from third-party platforms and partners in order to improve our services, conduct analytics, and better understand how our services are used, • to respond to court orders and legal investigations, respond to requests from public and governmental

determine whether individuals' interests outweigh our interests in the processing taking place. You can obtain more information about this balancing test by using the contact details in the Section "How to contact us".	authorities and cooperate with law enforcement, where we are permitted, but not legally required, to do so and where the processing is necessary and proportionate, including to establish, exercise or defend legal claims or protect the rights, safety and security of MoneyGram, our customers or others , • to analyze, improve and optimize Services and to understand traffic patterns and operations on our digital platforms, • to personalize your experience when you use Services, and to personalize content and ads where permitted by applicable law and subject to any consent, cookie choices, opt-out rights or other preferences that apply, • to respond to your queries that are unrelated to the Services, • to ensure the security and integrity of our technology, systems and Services, • to enforce our terms and conditions, • to associate you with different devices that you may use, including for fraud-protection purposes and personalization of content and ads, • to ensure the safety and security of our employees, customers, visitors, premises, systems, information and property, including by using CCTV where appropriate and permitted by law, • in connection with the sale, assignment or other transfer of all or part of our business in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, and • for the purposes of general business management and operations, and MoneyGram's internal administration, including agent relations management, personnel

	management, statistics and internal reporting within MoneyGram. We have an interest in ensuring the quality and safety of our Services, improving Services, and protecting our business interests and legal rights.
Your consent - in certain cases, we ask for your consent to use your data. Whenever we ask for your consent, we will explain the situations where we use your data and for what purposes.	• for the purposes described in the consent we obtain from you, • if required by applicable data protection laws, to send you marketing communications (via email, SMS or push notification) including offers, promotions, coupons or incentives we believe may be of interest to you, • to allow you to participate in sweepstakes, contests and similar promotions, and to administer these activities, • to receive data about you from social media platforms and advertising partners (such as Meta) where you have engaged with our advertising or content on those platforms, and to use that data to deliver personalised or interest-based advertising to you, including through custom audience and lookalike audience features, subject to your preferences and any opt-out rights that apply • to display or deliver interest-based ads where required by applicable law, including through cookies and similar technologies, and subject to your consent, cookie choices or opt-out rights where applicable, • to synchronize your contact list with your account, and • to connect your account to a third-party platform.

If you do not provide personal data that is necessary to provide a requested Service, verify your identity, comply with a legal obligation, manage risk or perform our contract with you, we may be unable to provide or continue providing the relevant Service, complete a transaction, maintain your account, or comply with applicable law.

How Do We Send Marketing Communications?

MoneyGram Global Privacy Notice

Last Updated October 2026

The rules for marketing communications depend on your location, the communication channel and your relationship with us. We distinguish between service messages and marketing messages.

Service and administrative messages

We may send you non-marketing messages that are necessary to provide or administer the Services, including transaction confirmations, security alerts, fraud-prevention messages, service updates, account notices, changes to terms, and loyalty-program administration messages. These messages are not promotional marketing and may be sent even if you opt out of marketing, unless applicable law requires otherwise.

Marketing messages

We may send you marketing communications about MoneyGram products, services, offers, promotions, coupons, incentives, loyalty benefits or similar opportunities where permitted by applicable law. Depending on your country and the channel used, we may rely on your consent, the "soft opt-in" for existing customers, legitimate interests, or another lawful basis permitted by local law.

Consent Where consent is required, we will send marketing communications only if you have given valid consent. You may withdraw your consent at any time by using the unsubscribe mechanism in our communication, changing your account or app preferences where available, replying "STOP" to SMS where supported, or contacting us at PrivacyProgramOffice@MoneyGram.com.

Soft opt-in communications Where permitted by applicable law, if you are an existing customer, the MoneyGram legal entity that obtained your contact details in connection with a sale or use of a Service may use those contact details to send you marketing about its own similar MoneyGram products or services, provided that you were given a clear opportunity to opt out when your details were collected and you are given an easy opt-out in each subsequent message.

Push notifications and in-app marketing. Where required, we will ask for your permission before sending marketing push notifications. You can manage push-notification preferences through your device settings or app settings, where available. Changing device settings may not unsubscribe you from other marketing channels, such as email or SMS.

Loyalty-program communications.

If you are a member of the MoneyGram Plus Rewards™ loyalty program or another loyalty program, we may send you administrative communications needed to operate the program, such as information about your membership, points, rewards, account status or material program changes. Promotional loyalty offers and marketing communications will be sent only where permitted by applicable law and your preferences.

Opt-Out:

You can opt out of marketing communications at any time by using the unsubscribe link in our emails, replying "STOP" to SMS where supported, changing your MoneyGram profile or mobile-app preferences where available, or contacting us at PrivacyProgramOffice@MoneyGram.com. We may keep a suppression record to make sure we respect your opt-out request.

These communications are sent as part of your membership benefits and are necessary to deliver the services associated with the program.

5. Who do we share your personal data with?

We share your personal data with:

- Other companies in MoneyGram, in particular: MoneyGram International, Inc. (Texas, USA), MPSI, MIS and MoneyGram Poland Sp. z.o.o. (Warsaw, Poland), for the performance of Services, internal administration, compliance, fraud prevention, AML and sanctions screening, customer support, product development, security, technology operations, and regular reporting, including in the context of a business re-organization or group restructuring, for system maintenance support, and for data hosting. Depending on the purpose, MoneyGram companies may act as independent controllers, joint controllers or processors/service providers.
- Our third-party providers, the majority of whom process personal data on our behalf and in line with our instructions. These include IT service providers, providers of auditing and control services, legal services, recovery, printing, disposal of documents, postal and courier services, companies and organizations that provide fraud protection services, and our agents and third-party providers we use to market Services or provide you with personalized ads or interest-based ads where permitted by applicable law and subject to your choices where required.
- Social media platforms and advertising partners, including Meta, TikTok and YouTube, where we use social-media pages, plug-ins, pixels, advertising tools, audience tools, SDKs or similar technologies. These platforms may process personal data as independent controllers or, in some cases, joint controllers with us. Where we act as joint controllers with a platform, we have entered into a controllership arrangement with that platform consistent with applicable data protection law. Under those arrangements, the relevant platform is the primary point of contact for you to exercise your data subject rights in respect of that jointly controlled processing; you can do so via the platform's own privacy tools and processes. Further information about cookies, pixels, SDKs, advertising tools and similar technologies is available in our Cookie Notice and in the privacy notices of the relevant platforms.
- Buyers or other successors in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets.
- Law enforcement bodies, courts, court enforcement authorities, regulators, government authorities, tax authorities, financial intelligence units and other competent public authorities, where disclosure is required or permitted under applicable law, regulation, court order, subpoena, warrant, regulatory request or other valid legal process. This may include disclosures necessary to respond to government, regulatory, law enforcement or supervisory authority requests, or to comply with anti-money laundering, counter-terrorist financing, sanctions, fraud prevention, tax, reporting or other legal and regulatory obligations .

6. How do we transfer your personal data to third countries?

MoneyGram operates globally and, therefore, personal data may need to be transferred to countries outside of where it was originally collected.

MoneyGram's global headquarters are based in the United States, and several material functions, systems and support operations are operated from or supported in the United States. MoneyGram has implemented intra-group data sharing and processing arrangements to regulate intra-group data flows, and we include appropriate data-transfer terms in data-processing or data-sharing agreements with third-party vendors where required. Where we transfer personal data internationally, we do so in accordance with the requirements of applicable data protection laws. Where required, we rely on appropriate transfer mechanisms, which may include adequacy decisions, standard contractual clauses approved by the European Commission, the UK International Data Transfer Agreement or UK Addendum, intra-group data-transfer agreements, transfer risk assessments, supplementary technical and organisational measures, or other lawful transfer mechanisms available under applicable law. In limited cases, we may also rely on derogations or exceptions permitted by law, for example where a transfer is necessary to perform a transaction or Service you request. This may include transfers to countries that competent authorities, such as the European Commission or the United Kingdom, have recognized as providing an adequate level of personal data protection.

To learn more about our data transfers or to receive a copy of the appropriate safeguards we have adopted, please reach out to us using the contact details in the Section "How to contact us". We may redact commercially sensitive or confidential information from copies of safeguards where permitted by law.

7. How long do we retain your personal data?

We store your personal data as long as reasonably necessary to provide the requested Services and to fulfill applicable legal, accounting, tax, AML, sanctions, fraud-prevention, dispute-resolution, audit, regulatory or reporting obligations to establish, exercise or defend legal claims. The specific retention period depends on the type of personal data, the Service used, the country involved, the purpose of processing, and applicable legal or regulatory requirements. For example:

- transaction, identity-verification and compliance records may need to be retained for the period required by AML, sanctions, money-transfer, tax, accounting and financial-services laws;
- customer-support, complaints and dispute records may be retained for the period necessary to handle the issue and defend against potential claims;
- marketing data is generally retained until you withdraw consent or object to marketing, after which we may retain limited suppression data to respect your choice;
- cookie and online tracking data is retained as described in our Cookie Notice;
- CCTV is retained for a limited period unless it is needed to investigate an incident, comply with law or establish, exercise or defend legal claims; and
- biometric data, where used, is retained only for as long as necessary for the relevant verification, security or compliance purpose and as permitted by applicable law.

Once the applicable retention period has expired, your personal data is securely deleted or destroyed, or where deletion is not immediately practicable, isolated from further processing and deleted as soon as reasonably possible.

8. What are our information security standards?

We use a variety of appropriate physical, technical, organizational, and administrative safeguards to protect your personal data from unauthorized access, loss, misuse, disclosure, destruction or alteration. These measures may include, as appropriate, access controls, encryption, authentication, monitoring, logging, secure development practices, vendor due diligence, confidentiality obligations, incident-response procedures, and business-continuity measures. No method of transmission or storage is completely secure, but we work to protect personal data in a manner appropriate to the nature of the data and the risks involved. You also play an important role in protecting your personal data. Please safeguard your login information, including account username and password, authentication credentials, and other account access information, and do not share these with others. You should notify us immediately of any suspected unauthorized use of your account or the Services.

9. What are your choices and rights?

Depending on and subject to applicable laws, you may have certain rights regarding the personal data that we hold about you. These rights may include the following:

- access to and obtaining a copy of your personal data;
- rectification of your personal data if it is inaccurate or incomplete;
- restriction of the processing or erasure of your personal data (the right to be forgotten);
- data portability, where the processing is carried out by automated means and is based on your consent or necessary to perform a contract;
- objection to the processing of your personal data where we rely on legitimate interests;
- rights relating to automated decision-making, including the right not to be subject to certain decisions based solely on automated processing, and the right to request human intervention or contest a decision, where these rights apply under applicable law;
- withdrawal of your consent at any time; such withdrawal does not affect the lawfulness of processing data which was carried out before withdrawal;
- opt out of receiving marketing communications from us at any time;
- raise a concern or complaint directly with us at any time;
- where applicable, appeal our decision if we decline to act on your request;
- where applicable, opt out of the sale or sharing of personal data, targeted advertising, or certain profiling activities;
- where applicable, limit, opt out of or withdraw consent to certain processing of sensitive personal data;
- where applicable, lodge a complaint with a data protection authority or other competent regulator; and
- where applicable, not be discriminated against or retaliated against for exercising your privacy rights.

If the applicable laws in your country provide different or additional data protection rights, you are entitled to exercise those rights in accordance with those laws. We will endeavor to respond to your request within the applicable statutory deadline, but our response time may vary depending on the applicable laws and your location. In some circumstances, we may be entitled to extend this period after notifying you. To respond to your request, we may need to confirm your identity. For that purpose, we may ask you for specific information or authenticate you in another way. We will not ask for more information than is reasonably necessary to verify your identity and process your request. Some requests, such as certain marketing opt-outs or opt-outs from sale or share under applicable U.S. state privacy laws, may not require identity verification.

Please note that there can be situations in which MoneyGram will be unable to fulfill your request. For example, MoneyGram may not be able to delete your personal data if those data are still required for the purposes for which they were initially collected and processed, such as the need to retain certain personal data to comply with legal, regulatory, reporting, anti-money laundering, sanctions, fraud-prevention, or legal claims obligations.

To exercise those rights, use the contact details in the Section "How to contact us".

10. How to submit a complaint to a supervisory authority?

Data protection laws vary across the jurisdictions. In most countries, you are entitled to lodge a complaint with a relevant authority in your country (where you live, work or where the suspected privacy issue occurred), if you are concerned about processing of your personal data or if your rights have not been complied with. However, we would like to encourage you to reach out to us first to share your questions or concerns or to exercise your rights. For that, you may use the contact details in the Section "How to contact us".

11. Do we make automated decisions or use profiling?

In some jurisdictions, we use automated systems as part of our Know Your Customer (KYC), identity verification, and financial crime compliance processes. These systems analyse information you provide and information obtained from trusted third-party sources to verify identity, assess risk, and meet our legal obligations (including anti-money-laundering and counter-terrorist financing requirements). Some of these processes may involve solely automated decision-making, including profiling, where permitted by applicable law, which may produce legal or similarly significant effects, such as the acceptance, restriction, or refusal of our services. Our automated systems work by comparing the information and documents you provide with trusted data sources, checking for inconsistencies or risk indicators, and screening against fraud-prevention, sanctions, and anti-money-laundering criteria. Based on a combination of these factors, the system generates an automated outcome (for example, verification successful, additional checks required, or verification unsuccessful), which may result in acceptance, restriction, a request for further information, or refusal of service. These processes rely on predefined rules and statistical or machine-learning models that assess multiple factors together; no single element is determinative on its own. Where required by applicable law, you may have rights relating to automated decision-making, including the right to request human intervention, express your point of view or contest a decision.

MoneyGram Global Privacy Notice

Last Updated October 2026

12. How do we notify you about changes to this Notice?

We reserve the right to update this Notice at any time. The updated Notice will be available on the website. The updated Notice will be available on the website and will indicate the effective date or last updated date. We will notify you directly of substantial updates that affect you where required by law or where the changes materially affect how we use your personal data.

13. How to contact us?

If you have any questions about this Notice or our privacy practices or would like to exercise any of your data protection rights, please:

- email us at PrivacyProgramOffice@MoneyGram.com
- submit your query via a dedicated intake form,

and we will assist you.

You may also contact us at our registered address, as provided in the controller list or applicable local supplement. However, we encourage you to contact us first using one of the options above.

14. Local supplements

The notices below supplement this Notice in line with the applicable data protection laws in those countries / regions and apply to individuals in those countries / regions.

A. Turkey

1. Who is the data controller?

Please click here to see details of the data controller in Turkey, for the purposes of the data protection laws applicable in Turkey, including *the Law on Protection of Personal Data No. 6698 of 7 April 2016* (the "**Law**").

2. Why do we collect, use and store your personal data?

We collect and process your personal data by automated, semi-automated, and non-automated means to the extent that such processing forms part of a data filing system, for the purposes and legal bases described in this Privacy Notice, as adapted by Section 4 below.

3. What are your choices and rights?

Our processing of your personal data is subject to applicable local law, and where the main Notice conflicts with the Law, the Law prevails. Accordingly, the rights described in Section 9 of the main Notice (in particular access, rectification, erasure, and rights relating to automated decision-making) apply to you as set out in Article 11 of the Law, and we will respond to your applications within 30 days of receipt, free of charge, unless your request involves a cost, in which case we may charge a fee in accordance with the tariff set by the Personal Data Protection Board. :

In Turkey, the following points apply to, or add to, the rights described in Section 9:

- your right to learn whether, and how, your personal data has been processed extends to knowing the specific third parties in Türkiye or abroad to whom your personal data has been transferred;
- where you request correction, erasure or destruction of your personal data, you may additionally request that we notify third persons to whom your personal data has been transferred of that correction, erasure or destruction;
- your right relating to automated decision-making under Article 11 is the right to object to a result that is against your interest, arising from analysis of your personal data solely through automated systems; and
- in addition to the rights described in Section 9, you have the right to demand compensation for damage suffered as a result of unlawful processing of your personal data.

Before applying to the Personal Data Protection Board with a complaint, you must first submit your request to us using the contact details in the "How to contact us?" section and either receive our response or allow 30 days to pass without a response, in accordance with Articles 13 and 14 of the Law. Only after this step may you apply to the Board.

4. Application and Interpretation of the Global Privacy Notice

Under the “Why do we collect, use and store your personal data” section above,

- the “Legitimate business purposes” legal basis is interpreted as our data controller’s legitimate interest, provided that the processing does not violate your fundamental rights and freedoms, and not that of others.
- where this Privacy Notice refers to “Your consent”, we will rely on your explicit consent, freely given, specific, informed and unambiguous, where required under the Law. Where explicit consent is required, we will provide information about the relevant processing purpose and request your consent separately from other terms and consents. Such purposes may include: personalizing content and ads, if required; sending you marketing communications (via email, SMS or push notification) including offers, promotions, coupons or incentives we believe may be of interest to you; allowing you to participate in sweepstakes, contests and similar promotions, and administering these activities; displaying or delivering interest-based ads; synchronizing your contact list with your account; and connecting your account to a third-party platform.
- where the main Notice describes processing of sensitive personal data (special categories of personal data under Article 6 of the Law, such as biometric data), such processing will be based on your explicit consent, or another basis specifically permitted under Article 6 of the Law.

We will notify you in the event of a new processing purpose in line with the Law.

5. Cross-border transfers of your personal data

Where your personal data is transferred outside Turkey, we do so only on one of the following bases, as required by Article 9 of the Law (as amended in 2024):

- the transfer is made to a country that the Personal Data Protection Board has recognized as providing an adequate level of protection;
- the transfer is made subject to a standard contract approved and published by the Board, executed with the overseas recipient, and notified to the Board within five business days of signature; or

- the transfer is made under a binding undertaking approved by the Board, or another mechanism or exception permitted under Article 9.

We do not rely on the EU Standard Contractual Clauses or UK transfer mechanisms described in Section 6 of the main Notice as a basis for transfers out of Türkiye; those mechanisms apply to transfers governed by EU/UK law only.

6. Complaints

If you are not satisfied with our response to your application, you may lodge a complaint with the Personal Data Protection Board (Kişisel Verileri Koruma Kurulu), provided you have first applied to us in accordance with Section 3 above. Contact details for the Board are available at www.kvkk.gov.tr

B. Mainland China

1. What are the categories of your sensitive personal data which we process?

Sensitive personal data refers to personal data that, if leaked or used illegally, may easily lead to an infringement upon the human dignity of a natural person or the harm of the safety of his/her body or property.

Sensitive personal data that we may process may include:

- your national identification number(s) and national ID details;
- your facial image and other biometric information;
- your social security or other taxpayer identification number(s);
- your banking details, financial account information, payment information and account or wallet-related information;
- your location information or whereabouts; and
- where applicable, personal information of minors under the age of 14.

We process sensitive personal data only where it is necessary for a specific purpose and we have obtained your separate consent (单独同意), or another legal basis for processing sensitive personal data permitted under the Personal Information Protection Law ("PIPL"), and we will inform you of the necessity of the processing and its impact on your rights and interests before doing so.

2. What is the legal basis for processing your personal data under Chinese law?

Chinese law does not recognize "legitimate interest" as a standalone legal basis for processing. Where the main Notice describes a purpose as based on our legitimate business purposes, in Mainland China we instead rely on one or more of the following bases, as applicable to that purpose, consistent with Article 13 of PIPL:

- your separate consent, obtained specifically for that purpose;
- the processing is necessary to conclude or perform a contract to which you are a party, or necessary for human-resources management in accordance with labor rules and collective contracts (as applicable);
- the processing is necessary to perform statutory duties or statutory obligations, including anti-money-laundering, counter-terrorist-financing and sanctions obligations;

- the processing is necessary to respond to a public health emergency, or to protect the life, health or property safety of a natural person in an emergency;
- the processing is carried out within a reasonable scope of personal data that you have already made public, or that has otherwise been lawfully made public, in accordance with PIPL.

Where none of the above applies to a purpose described as "legitimate business purposes" in the main Notice (for example, delivering personalized ads), we will obtain your separate consent before carrying out that processing in Mainland China.

3. How do we transfer your personal data outside Mainland China?

Where we transfer your personal data outside Mainland China, we do so on one of the following bases, as required by Article 38 of PIPL:

- passing a security assessment organized by the Cyberspace Administration of China ("CAC"), where required based on the volume or type of data involved;
- obtaining personal information protection certification from a CAC-recognized professional institution;
- entering into a standard contract with the overseas recipient in the form formulated by the CAC, and filing that contract with the provincial-level cyberspace administration; or
- another mechanism permitted by law or by the CAC.

Before transferring your personal data outside Mainland China, we will inform you of: the name and contact details of the overseas recipient; the purpose and method of processing by the overseas recipient and the categories of personal data involved; the way in which you may exercise your rights against the overseas recipient; and other matters required by law, and where the transfer is based on consent, we will obtain your separate consent to the cross-border transfer.

4. What are your choices and rights?

In Mainland China, the following points apply to, or add to, the rights described in Section 9:

- our right to data portability under Section 9 is the right to request that we transfer your personal data to another personal information processor designated by you, where the conditions required by law are met;
- your rights relating to automated decision-making under Section 9 include the right to request that we explain the logic of a decision made about you, and to refuse a decision made solely through automated means, where that decision has a significant impact on your rights and interests;
- in addition to the rights described in Section 9, you have the right to know about and decide on our processing of your personal data generally, including the right to restrict or refuse processing, and the right to ask us to explain our personal data processing rules; and
- in addition to the rights described in Section 9, you have the right to refuse or opt out of the use of your personal data for direct marketing, personalized recommendations, or other commercial communications, where applicable.

We will respond to a request in which you exercise your data protection rights within 15 business days, extendable by a further 15 business days where necessary, with notice to you of the extension and the reason for it.

5. Complaints

You may lodge a complaint or report regarding our processing of your personal data with the Cyberspace Administration of China or the relevant local cyberspace administration department, or with another department performing personal information protection duties, in accordance with Article 65 of PIPL.

C. Hong Kong

1. Direct marketing

Before we use your personal data for direct marketing for the first time, or provide your personal data to a third party for the third party's direct marketing, we will, in accordance with the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"):

- inform you of the kinds of personal data we intend to use for direct marketing;
- inform you of the kinds of products or services to which the marketing relates;
- where we intend to provide your personal data to a third party for the third party's own direct marketing, inform you of the classes of persons to whom the data may be provided, and obtain your written consent (which may include consent given electronically) before doing so; and
- inform you that we may not use your personal data for direct marketing, and may not provide it to a third party for that purpose, unless we have received your consent (or, where permitted, an indication that you do not object), and that you may do so without charge.

The soft opt-in, legitimate-interest and consent mechanisms described in the "How Do We Send Marketing Communications?" section of the main Notice do not apply to direct marketing carried out in or into Hong Kong; this Section 1 applies instead.

2. What are your choices and rights?

In Hong Kong, the rights described in Section 9 of the main Notice apply to you only to the extent set out below. Under the Personal Data (Privacy) Ordinance (Cap. 486), you are entitled to:

- request access to your personal data, including a copy of it;
- request correction of your personal data if it is inaccurate; and
- if we refuse to correct your personal data as requested, request that we attach to the personal data a note of the correction you sought, and take reasonably practicable steps to forward that note to any third party to whom the data was previously disclosed, where you so request.

We will respond to your requests within 40 days of receipt, in accordance with the PDPO. We may charge a fee for complying with a data access request, to the extent permitted by the PDPO; we will not charge a fee for a data correction request.

3. Complaints

If you are not satisfied with our response, you may lodge a complaint with the Office of the Privacy Commissioner for Personal Data, Hong Kong ("PCPD"). The PCPD's contact details are available at www.pcpd.org.hk.

MoneyGram Global Privacy Notice

Last Updated October 2026

D. U.S. State Privacy Supplement

If you are U.S. resident outside California, please review our United States Privacy Notice for additional information about our privacy practices in the United States, including the specific rights available under the comprehensive consumer privacy laws of the state in which you reside.

If you are a California resident, please review MoneyGram Privacy Notice for California Residents for additional information about our collection, use, disclosure, sale, and sharing of personal information under the California Consumer Privacy Act ("CCPA"), including your right to receive an annual disclosure of the categories of personal information we have disclosed to third parties for their direct marketing purposes in the preceding calendar year, at no charge, in accordance with California's "Shine the Light" law.

Where you reside in a state with a comprehensive consumer privacy law (including, as applicable, Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, Florida, Delaware, Iowa, Indiana, Tennessee, New Jersey, Maryland, Minnesota, Nebraska, New Hampshire, Kentucky, and Rhode Island, among others), our United States Privacy Notice describes, as applicable in your state:

- your rights to access, correct, delete and port your personal data, and to opt out of targeted advertising, the sale of personal data, and profiling in furtherance of decisions that produce legal or similarly significant effects;
- how we recognize an opt-out preference signal, such as the Global Privacy Control, where required by your state's law, as an exercise of your right to opt out of targeted advertising and the sale of personal data;
- our practices regarding sensitive personal data, including that we will seek your consent before processing sensitive personal data where required by your state's law;
- how you may designate an authorized agent to submit a request on your behalf; and
- your right to appeal a decision we make in response to your request, and how to do so, where required by your state's law.

E. Australia and New Zealand

This Australia and New Zealand supplement applies where you use MoneyGram Services in Australia or New Zealand. It supplements the information provided in this Privacy Notice, and where the main Notice conflicts with the Privacy Act 1988 (Cth), the Privacy Act and this supplement prevail.

1. Australia — your Privacy rights

The Privacy Act and the Australian Privacy Principles ("APPs") override the rights described in Section 9 of the main Notice in relation to our handling of your personal information in Australia. The Privacy Act does not provide a standalone right to erasure or data portability in the form described in Section 9. Instead, under the APPs you have the right to:

- access the personal information we hold about you (APP 12);
- request correction of personal information that is inaccurate, out of date, incomplete, irrelevant or misleading (APP 13);
- request that we not use or disclose your personal information for direct marketing purposes, and that we identify the source from which we obtained your personal information for direct marketing (APP 7); and

- complain about a breach of the APPs, as described below.

2. Australia — privacy complaints and OAIC contact details

If you are in Australia and have a privacy question, concern or complaint, we encourage you to contact MoneyGram first using the contact details in the main Notice.

If you are not satisfied with our response, or if you wish to contact the Australian privacy regulator, you may contact the Office of the Australian Information Commissioner ("OAIC"). The OAIC's complaint guidance states that individuals can seek help lodging a privacy complaint by emailing oaicintake@oaic.gov.au or calling the OAIC Enquiries Line on 1300 363 992.

3. New Zealand – your Privacy rights

The Privacy Act 2020 and the Information Privacy Principles ("IPPs") override the rights described in Section 9 of the main Notice in relation to our handling of your personal information in New Zealand. The Privacy Act 2020 does not provide a standalone right to erasure or data portability in the form described in Section 9. Instead, under the IPPs you have the right to:

- request confirmation of whether we hold personal information about you, and to access that information (IPP 6); and
- request correction of your personal information (IPP 7).

4. New Zealand — privacy complaints and Privacy Commissioner contact details

If you are in New Zealand and have a privacy question, concern or complaint, we encourage you to contact MoneyGram first using the contact details in this Privacy Notice.

If you are not satisfied with our response, or if you wish to contact the New Zealand privacy regulator, you may contact the Office of the Privacy Commissioner. The Commissioner states that individuals should generally complain directly to the relevant organisation first, and that complaints can be made through the Commissioner's complaints page. The Office of the Privacy Commissioner can also be contacted by phone on 0800 803 909.