

Ria Money Transfer Privacy Notice

Version 3.2 - January 2026

This Privacy Notice explains how we process your Personal Data when you engage with our services, whether by browsing our website or mobile application, completing transactions, visiting our establishments, or interacting with us in any other way. It also details how we may share your Personal Data with third parties and the safeguards we have implemented to protect your information.

References to “we,” “us,” and “our” in this Privacy Notice refer to **Ria**, a segment of Euronet Worldwide. The specific legal entity acting as the Data Controller is listed in Our Companies section.

We recommend reviewing this Privacy Notice regularly for updates, which will be posted on our Website/App. Where local laws require additional information, these are provided in the Regional Privacy Notices section.

To reach the Privacy Department or the Data Protection Officer (DPO)

- Email: dpo@riamoneytransfer.com
- Postal mail: DPO, Calle Cantabria 2, 2-A Alcobendas Madrid, Spain

If you are an Authority, please reach out to us to the following address

- Ria-Compliance@riafinancial.com

Frequently Asked Questions (FAQs)

What Personal Data do we collect?

We only collect the Personal Data necessary to provide our services and comply with legal obligations. The specific categories of Personal Data collected may vary depending on the service or interaction.

From where do we obtain your data?

We collect Personal Data mainly from you, when you interact with our company and services. However, we may collect additional data to fulfil our obligations from other sources.

Why do we collect Personal Data?

We collect Personal Data to comply with our obligations with you and to comply with our legal obligations. We process your Personal Data to ensure the delivery and security of our services and/or improve our operations. Whenever we process your Personal Data for additional purposes, we will make sure to inform you and, when necessary, gather your consent.

For how long do we retain Personal Data?

We retain Personal Data only for as long as necessary to fulfill the purposes for which it was collected, including the provision of services, compliance with legal obligations, or the exercise or defense of legal claims. Once Personal Data is no longer required, we securely delete or anonymize it in accordance with applicable laws.

With whom do we share Personal Data?

We may share Personal Data with Euronet Group companies, legal authorities, and selected third parties/partners when required to meet regulatory standards or fulfill contractual commitments.

Where is Personal Data stored?

We store Personal Data in secure facilities with stringent security controls. Any international transfer of Personal Data complies with all legal obligations and maintains the highest security standards.

What are your rights regarding Personal Data?

Depending on your location, you may have specific rights concerning your Personal Data under applicable laws. Common rights are described under the section “Your Rights”.

Notice to Website visitors

By visiting or using our Website, you acknowledge that you have read, understood, and agree to be bound by this Privacy Notice. You should not provide us with any of your information if you do not agree with the terms of this Privacy Notice.

To the extent this Website allows access to other websites owned and operated by third parties, please note that this Privacy Notice will not apply to such websites, and thus, we will not be held responsible for the protection of personal data processed by these third parties.

What Type of Personal Data Do We Collect?

The categories, purposes, and legal bases for collecting and processing your Personal Data when you visit and/or use our Website are listed below. Where the collection and processing of Personal Data is based on your consent, you may withdraw your consent at any time.

Identification and contact data

This may include name, email, phone number, address, title, and other contact details. It may also include data you voluntarily provide during chats, calls, or written correspondence.

Purposes and Legal Basis for Processing

- **Service Provision:** To manage your online inquiry via the Website form (i.e. registering your inquiry, contacting you, processing and responding to your inquiry). This processing is carried out based on our pre-contractual and/or contractual obligations.
- **Legal Claims and Archiving:** To pursue any legal claims, as well as for archival purposes related to this purpose, including securing information in the event of the need to prove facts, when necessary to protect our legitimate interests.
- **Marketing:** To provide advertising and marketing, including measuring the impact of our emails, based on your consent.
- **Giveaway Participation:** To manage your participation in events or giveaways, based on your consent.
- **Regulatory Compliance:** To comply with applicable laws, regulatory obligations, and decisions by competent authorities. This processing is required to meet our legal obligations.

Behavioral and Technical Information

Information collected through cookies or other tracking technologies such as IP address, network activity, browsing behavior, browser type, time zone, screen resolution, plug-ins, operating system, device signature, and technical characteristics.

For more information, please read our Cookie Policy.

Purposes and Legal Basis for Processing

- **Website Security and Integrity:** To ensure the efficient operation, management, safety and security of our Website. Please note that, amongst other safeguards, we have tools to protect our Website for the purposes of fraud prevention and security controls. This processing is based on our legitimate interest.

- **Website Maintenance and Improvement:** To undertake activities to verify or maintain the quality of the Website, and to improve, upgrade, or enhance the Website, including to administer the Website for internal operations, such as troubleshooting, data analysis, testing, research, statistical and survey purposes. This processing is based on our legitimate interest.
- **Usability Tracking and Testing:** To track detailed user activity across the Website or other platforms (e.g. which buttons are clicked, how far pages are scrolled, etc.). These tools allow us to understand how visitors interact with our content and features, enabling us to test improvements and optimize usability. This tracking is cookie-based and implemented under our legitimate interest in improving our services and user experience. Where required by applicable law, we obtain your consent before activating such tracking technologies.
- **Personalization:** To measure and evaluate your behavior using automated processing to provide you with a more personalized Service. This processing activity is based on your consent.

Location Data

- **Service provision:** We may collect information about your location when you visit our Website. This does not include your exact location. This information is processed based on our legal obligations.
- **Nearby Locations:** We may collect information about your location when you visit our Website to show you our nearest locations. This information is based on your consent.

Non-identifiable Data

Whenever possible, we use data where you cannot be directly identified (such as anonymous demographic and usage data) rather than Personal Data (“Non-identifiable Data”). This Non-identifiable Data may be used to improve our internal processes or delivery of services, without further notice to you. We may use aggregate data for a variety of purposes, including analyzing, evaluating and improving our Website and its content.

Notice to Money Transfer, Currency Exchange, Bill Payment and Check Cashing Users

This Privacy Notice applies to individuals using Ria’s financial services, including:

- **Money Transfer:** Enabling you to send or receive funds.
- **Currency Exchange:** Providing the ability to exchange one currency for another.
- **Bill Payment:** Allowing payment of utility bills, phone top-ups, and other recurring obligations.
- **Check Cashing:** Facilitating the cashing of checks issued in your name.

What Type of Personal Data Do We Collect?

Identification Data

We collect identification data, such as your name, email, phone number, address, date of birth, gender, images, videos, and signature. We also process sociodemographic data such as age, marital status, family situation, residences, education and occupation (type of contract, type of occupation, employer), level of education and professional experience.

Purposes and Legal Basis for Processing:

- **Service Provision:** To deliver our services, based on our contractual obligations.
- **Customer Service:** To provide customer service, based on our contractual obligations.
- **Record of Conversations:** We will monitor and record (via automated means or transcripts) our telephone calls, emails, and chat conversations with you, on any platform, to confirm the instructions provided to us. This is based on our legitimate interest.
- **Account Management:** To manage your account(s) (i.e.: registration, administration, maintenance and servicing accounts). This processing is necessary for the performance of a contract.
- **Marketing:** To provide advertising and marketing. This processing is based on your consent.
- **Giveaway Participation:** To manage your participation in events or giveaways. This processing is based on your consent.
- **Regulatory Compliance:** To fulfill legal obligations, including retention requirements.

- **Identity Verification:** In very limited circumstances, to perform a credit check for identity verification. This processing is necessary to comply with legal obligations.
- **Market research & consumer feedback:** To analyse any information that you voluntarily share with us about your experience of using our products and services. This processing is based on consent.

Financial Information

To provide our services, we collect financial information such as bank details and transaction purposes.

Purposes and Legal Basis for Processing:

- **Service Provision:** For transaction processing. This processing is necessary for the performance of a contract.
- **Regulatory Compliance:** For anti-money laundering and anti-terrorist financing. This processing is necessary to comply with legal obligations.
- **Account Management:** To manage your account. This processing is necessary for the performance of a contract.
- **Credit Checks:** In very limited circumstances, to perform a credit check in order to provide the Services. This processing is necessary to comply with legal obligations.
- **Identity Verification:** To verify the customer's identity (i.e., KYC: for additional information [click here](#)). This processing is necessary to comply with legal obligations.

We will never ask you to provide your payment information (i.e., credit/debit card details). None of our employees or agents will ever ask for your payment information. Where payment information is required, we will ask you to enter the information directly into secure payment processing systems managed by authorized third-party payment processors (which may include Euronet group affiliates). These processors handle the data in compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Transactional Data

We collect personal data like the beneficiary details, bank account information, contact information, the destination where you are sending money and bank preferences. Depending on the local regulation, we may also collect details such as the relationship with the beneficiary, transfer reason and additional documentation related to the transaction.

Purposes and Legal Basis for Processing:

- **Service Provision:** To provide the Services, including completing a transaction. This processing is necessary for the performance of a contract.
- **Regulatory Compliance:** For compliance purposes related to a transaction. This processing is necessary to comply with legal obligations.

Location Information or Geolocation Data

We may collect information about your location when you use our Services.

Purposes and Legal Basis for Processing:

- **Nearby locations:** To provide the Service, including using device location to identify nearby locations for pick-up and drop-off. This processing is based on your consent.
- **Service Provision:** We need to know the country you are based in order to provide you with our services. This processing is necessary to comply with legal obligations. Note that we will never have your exact location, only the country of origin.

Audio and Video Surveillance

We may utilize CCTV footage (image, video, and audio/voice recording) to ensure safety in our stores or offices in compliance with local regulations. The retention period of the recordings shall not exceed the duration mandated by our legal obligations.

Purpose and Legal Basis for Processing:

- **Security:** To maintain safety in our stores or offices. This processing activity is based on our legitimate interest, or where required by local regulations, to comply with legal obligations.
- **Fraud Prevention:** Where permitted by local regulation, we may access CCTV content to verify transactions, prevent fraudulent activities, and protect our assets and our customer rights. This processing is necessary to comply with legal obligations.

Sensitive Personal Data

When strictly necessary, we may collect sensitive data, such as biometric data (e.g., face scans), government ID numbers, and health information, in compliance with local laws. Where required by applicable law, we will obtain your consent or present you with an opportunity to opt out before processing your Sensitive Personal Data.

Purposes and Legal Basis for Processing:

- **Legal Compliance:** For KYC and fraud prevention. This processing is carried out to comply with legal obligations.
- **Security and Verification:** To verify identity during service use. This processing activity is carried out to comply with our legal obligation. When required, we will ask for your consent.

Non-Identifiable Data

When possible, we use non-identifiable data to enhance services, such as anonymous demographics or aggregated usage data.

Personal Data of a Beneficiary

For money transfer services, Personal Data of beneficiaries is collected from customers, as it is essential to fulfill the contractual agreement between us and our customer. As the beneficiary, you are the recipient of the payment transaction initiated by our customer.

The types of Personal Data we may collect about you include:

- **Identification Data:** Name, surname and government ID.
- **Financial Data:** Bank information or payout information like wallet, card or mobile number.

We process the Personal Data of a beneficiary exclusively to meet our contractual and regulatory obligations.

In some cases, we may contact you, the beneficiary, to inform you of a transaction in progress that requires your attention and action. We will never contact you to promote our services but only to comply with our contractual or legal obligations.

Your data, as a beneficiary, will not be used for other purposes.

If you have questions about how we process your Personal Data as a beneficiary, please contact us at dpo@euronetworldwide.com.

Know Your Customer (e-KYC) process

For our digital services, and where legally permitted and required, we may verify your identity using an electronic Know Your Customer (e-KYC) process. This may involve submitting a valid photo ID, video or selfie through our secure service provider's platform. This process enhances fraud detection and ensures compliance with anti-money laundering regulations.

When biometric data, such as face scans, is collected, we will request your consent if required by local law. If you prefer not to provide biometric data, please contact our customer care team for assistance.

During the verification process, a video, including audio, may be recorded to ensure the integrity of the procedure. All biometric data shared with our service providers is carefully controlled and used strictly for identity verification purposes. Neither we nor our service providers will sell, lease, or trade your biometric information, and robust security standards are maintained to prevent unauthorized access.

In line with applicable privacy laws, you may have rights regarding your biometric data, such as access rights. For more information, refer to the “Your Rights” section. For questions about the e-KYC process, contact us at dpo@euronetworldwide.com.

RIA Rewards Program

What Type of Personal Data Do We Collect?

If you choose to enroll in our RIA Rewards Program (where available), we will process your Personal Data as follows:

Identification Data

Identification Data may include your name, title, residential and/or business address, email, phone numbers, date of birth, gender, images, signature, passport or visa details, voice recordings, and official credentials. We use only the Identification Data strictly necessary for the purposes outlined below:

Purposes for Processing Your Personal Data

- **Service Provision:** To perform and deliver services. This processing is necessary to fulfil our contractual obligations.
- **Customer Service:** To monitor and record communications (e.g., calls, emails, chats) for confirming instructions. This processing is based on our legitimate interest.
- **Account Management:** For registration and account administration. This processing is required to fulfil our contractual or pre-contractual obligations.
- **Access to Tools and Information:** To provide requested tools and information via the App for Services like foreign exchange and payments. This processing is required to fulfil our contractual or pre-contractual obligations.

- **Correspondence and Record Keeping:** We retain communication records and customer service interactions for service support, alongside communications with Euronet Group affiliates and partners. This processing is based on our legitimate interest.
- **Market research & consumer feedback:** To analyse any information that you voluntarily share with us about your experience using our products and services. This processing is based on consent.

Transactional Data

We collect information on transaction details, such as the amount and destination of transfers, to award points under the Rewards Program.

Purpose for Processing Your Transactional Data

- **Rewards Points:** To allocate points based on eligible transactions. This processing is required to fulfil our contractual obligations.

Contact Information for Rewards Program

To withdraw from the program, report suspicious or unauthorized activity, or update your preferences, you can contact the Rewards Program at:

- toll-free number **1800 882 077** during business hours or
- by email at riarewards@riamoneytransfer.com

Toll-free calls are free from landlines, but charges may apply from mobile phones based on your provider.

If you have opted to receive marketing communications from us, we will keep you informed when Rewards becomes available in your country.

General Notice

Where do we obtain your Personal Data?

We collect Personal Data mainly from you when you interact with our company and services. However, we may collect additional data from the following sources:

- Passive collection on our websites, including information about your page clicks, time spent, and other automatically gathered metadata.
- Advertising networks and social media platforms.

- Service providers, including but not limited to data analytics providers, internet service providers, operating systems and platforms, and other third parties that support the delivery, operation, security or analysis of our services.
- Other Parties such as government databases, business partners and third-party sources

Personal Data Collected from Other Parties

We may collect your Personal Data from other sources, depending on the service and local legal requirements. These third-party sources include:

Authorities and Public Records

We may obtain Personal Data from public record sources (such as federal, state, or local government organizations) in order to comply with legal obligations and ensure the accuracy of the information we hold.

Purposes for Processing:

- **Identification purposes:** We may check the Personal Data you have provided us with our third parties to make sure your identity matches the information you have provided us. The legal basis for this processing is our legal obligation.
- **Fraud prevention:** We may compare data collected from you with data provided by third parties for fraud prevention, including impersonation, misuse of services, or other suspicious activity.

Business Partners and Other Third Parties

We may also obtain your Personal Data (such as name, email, phone number, employer) from our business partners and other third parties. Any Personal Data obtained from these sources is processed only for specific legitimate purposes and in accordance with applicable data protection laws. These parties are responsible for collecting your consent when sharing your Personal Data with us, if applicable. However, if you believe we should not have your Personal Data, you can request your deletion at dpo@euronetworldwide.com.

Purposes for Processing:

- **Service delivery and support:** We may process your data to ensure we can provide you with seamless experience, especially when our services are offered through our business partners and clients as part of integrated or partner-branded solutions.
- **Promotion of our services:** To provide you with information about our products or services, where permitted by law and based on your consent, if required.

- **Business Development:** To maintain and develop business relationships and ensuring relevant and accurate communication with potential and existing business partners. This processing is based on consent.

If we process any additional data obtained from a third party, we will inform you as soon as possible and obtain your consent where required by applicable law.

How Long We Keep Personal Data

We retain Personal Data only as long as necessary to provide requested services and to meet legal, accounting, and reporting obligations. The retention period is determined by specific requirements and may include:

- **Customer Service and Contractual Relationship:** We retain your Personal Data while you remain our customer. When our contractual relationship concludes, we restrict your data to ensure it is only accessible to comply with legal requirements.
- **Marketing:** We will process your Personal Data for marketing purposes unless you have opted out, as described in this Privacy Notice, or until we become aware that you are no longer interested, or that your data is no longer accurate.
- **Legal and Regulatory Requirements:** We keep your Personal Data as long as needed to comply with all applicable legal obligations, including commercial, tax, and anti-money laundering regulations. During this period, your Personal Data is restricted to prevent use for any other purpose and will be accessed only when necessary to fulfill these obligations.

Please note that if you request data deletion we may still be required to retain some of it to comply with our legal obligations. The information retained will only be accessible by limited personnel to comply with any legal requirement and will be dully deleted after the obligation is due.

Do We Disclose Personal Data?

Euronet Group Affiliates

We may disclose Personal Data to Euronet and its affiliated companies for everyday business purposes and fulfil compliance obligations within the Group.

Types of Personal Data: Identification Data, Video Surveillance, Transactional Data, Financial Details, Behavioral and Technical Data.

Purpose: Sharing data with affiliates for customer service, compliance, and daily business functions. This may include 24/7 customer support requiring data access across Euronet Group affiliates.

In the event of a sale, acquisition, merger, or reorganization involving Euronet or any company within the Euronet Group, we may transfer Personal Data to third parties, ensuring appropriate protection measures.

This processing is carried out to comply with legal obligations and/or to perform contractual obligations, as applicable.

Third-Party Service Providers

We may share certain Personal Data with third-party service providers to support compliance verification, service delivery, and marketing efforts.

Types of Personal Data: Identification and Biometric Data, Financial Details, Contact Details, Transactional, Behavioral, and Technical Data.

Purpose

- **Compliance and Fraud Prevention:** Personal Data may be shared with verification and analytics providers to fulfill regulatory obligations and mitigate risk (e.g., to verify customer data or detect suspicious activity). This processing is carried out to comply with our legal obligations or, where applicable, based on your consent.
- **Service Delivery:** Our Partners and third parties, such as agents and correspondents, may access Personal Data to assist in delivering services. This processing is based on our contractual obligation.
- **Marketing:** Advertising networks and social media platforms may receive data to deliver personalized ads and adapt to user preferences. This processing is based on your consent.

Note: The definition and scope of “third-party service providers” may vary based on country regulations.

Authorities

We may be required to disclose your Personal Data, including Sensitive Personal Data, to legal or regulatory authorities for compliance, to enforce agreements, or to fulfill legal requests.

Types of Personal Data: Identification Data, Video Surveillance, Transactional Data, Financial Details.

Purpose: To comply with applicable laws, respond to binding requests from public authorities, support investigations, or fulfill obligations related to the processing of financial transactions. This processing is based on our legal obligations.

Partners

Personal Data may be shared with strategic partners when necessary to deliver our services or to ensure they comply with their legal obligations.

Types of Personal Data: Identification Data, Transactional Data, Financial Details.

Purpose and Legal Basis for Processing

- **Purpose:** Service provision in collaboration with strategic partners. This is carried out as part of our contractual obligations.
- **Regulatory Compliance:** To help our partners comply with legal or regulatory requirements applicable to them. This processing is based on legal obligations.
- **Operational Efficiency and Risk Management:** To support secure and seamless service delivery across different partners or service providers, or to prevent abuse or misuse of our services. This processing is based on our legitimate interests.

Professional Partners

We may disclose Personal Data to professional advisors, including lawyers, consultants, auditors, or accountants, to fulfill our legal and business obligations.

Types of Personal Data, Identification Data, Video Surveillance, Transactional Data, Financial Details. (Legal obligation and Legitimate interest)

Legitimate Interest

When we use your Personal Data to pursue our legitimate interests, we will make every effort to match our interests with yours so that your Personal Data will only be used as permitted by relevant law, or when it will not adversely affect your rights. You may request information on any processing based on legitimate interest.

International Transfers

We are a global company with global operations, partners and suppliers. Where it is necessary for the efficient and effective performance of a business transaction or the fulfilment of one of the uses of Personal Data outlined above, we may need to transfer your Personal Data, from the country of collection to other countries, which may have data protection laws that are different from the laws where you live. When such transfer is required, we implement appropriate safeguards to ensure it receives the same level of protection and the transfer is done according to our legal obligations.

Personal Data of Minors

We do not provide services directly to minors, as defined by applicable local legislation, or proactively collect their personal information. If you are considered a minor under your local laws, ensure to have the necessary authorizations from your legal guardian to use the Sites or Offerings or share personal data with us.

If you learn that a minor has unlawfully provided us personal data, please contact us at dpo@euronetworldwide.com.

Security

We are dedicated to safeguarding your Personal Data and have implemented robust, commercially reasonable security measures to prevent its loss, misuse, or unauthorized alteration. We continuously work to protect your data in line with international best practices by applying rigorous physical, electronic, and managerial safeguards.

To prevent unauthorized access, we employ advanced physical and organizational security measures that are regularly updated to ensure the highest level of protection while maintaining cost efficiency. All Personal Data is stored in secure locations, protected by firewalls and other sophisticated security systems with restricted administrative access.

Our personnel, as well as all activities related to your Personal Data, are governed by strict confidentiality agreements that enforce compliance with our organization's Privacy Policy.

Our goal is to uphold the highest standards of data protection by industry-leading practices that safeguard your privacy.

Accuracy of Personal Data

We are committed to keeping your Personal Data accurate and up to date. We take reasonable steps to ensure the accuracy of your Personal Data by ensuring that the latest Personal Data we have received is accurately recorded and when considered necessary, we run periodic checks and request that you update your Personal Data.

You may request a correction or update to your Personal Data if it is inaccurate, as outlined in the Your Rights section below.

Your Rights

To exercise any of your rights, please email us at **dpo@euronetworldwide.com**. To safeguard your privacy and maintain security, we may ask you to verify your identity and provide additional information.

Depending on your location, your rights concerning Personal Data under applicable laws may include:

1. **Right to Know:** You have the right to know what Personal Data is collected, **sold**, or shared, and with whom.
2. **Right to Access:** You may request access to a copy of your Personal Data.
3. **Right to Correct:** You can request corrections to inaccuracies in your Personal Data.
4. **Right to Delete:** You may request deletion of your Personal Data under certain conditions.
5. **Opt-Out Rights:**
 - You may opt-out of the processing of Personal Data for targeted advertising.
 - You may opt-out of the processing of Sensitive Personal Data.
 - You may opt-out of the processing of Personal Data for profiling that leads to legal or significant effects on you.
6. **Right to Limit Use of Sensitive Data:** You may request to limit the use and disclosure of Sensitive Personal Data to specific, permitted purposes.
7. **Right to Restrict Processing:** You can request restrictions on data processing under certain conditions.

8. **Right to Object:** You may object to the processing of your Personal Data, for example, for direct marketing purposes.
9. **Rights Related to Automated Decision-Making:** You have the right not to be subject to decisions based solely on automated processing, including profiling, that produces legal or similarly significant effects.
10. **Right of No Retaliation:** You have the right not to face discrimination for exercising your Personal Data rights.

We will respond to your requests promptly and within the timeframe required by law. For specific rights in your jurisdiction, refer to the [Regional Privacy Notice section below](#).

Please note that some rights may not be enforceable due to business or legal requirements necessary to provide our services, such as anti-money laundering, contractual, or compliance obligations. However, we will always respond to any rights requests as outlined above, and you may have additional rights based on your location.

Privacy Complaints

If you have a complaint about how we process your Personal Data, please contact us at **dpo@euronetworldwide.com**.

Under applicable privacy laws, you may also have the right to lodge a complaint with a Data Protection Authority or other regulatory body if you believe we have not fulfilled our obligations under this Privacy Notice or the relevant legal requirements.

Access to your Device Features

We may request access to certain features on your device to enhance your experience and enable specific functionalities. Access to these features is optional and based on your prior consent:

- **Contact List:** through the App, we may access your contact names and numbers solely to allow convenient selection of beneficiaries. These contacts remain stored locally on your device and are not downloaded, processed, or used for any other purpose.
- **Camera and Microphone:** When necessary for identity verification (e.g., during e-KYC), the App may access your camera and microphone. These features are used exclusively to complete the verification process securely.

- **Location Services:** If enabled, your location may be used to tailor services such as identifying nearby branches or adapting content regionally.

You can revoke access to these features at any time through your device or App settings.

Use of Artificial Intelligence

We may use Artificial Intelligence (AI) and Machine Learning (ML) technologies, either developed internally or provided by trusted third parties—to assist with operational, regulatory, and compliance purposes across its global services.

The use of such technologies is strictly limited to the legitimate purposes outlined in this Privacy Notice and is implemented in a manner that respects individual rights and freedoms. Where required under applicable law, Euronet performs Data Protection Impact Assessments (DPIAs) to evaluate and mitigate any risks associated with the deployment of AI/ML systems.

These technologies do not make decisions that produce legal or similarly significant effects on individuals without appropriate human oversight. Where applicable, and in accordance with regional data protection laws, individuals have the right to:

- Request information about the existence and nature of any automated processing involving their data,
- Object to processing based solely on automated decision-making,
- Request human intervention or to express their point of view in such contexts.

Euronet maintains appropriate safeguards to ensure the transparency, accuracy, fairness, and security of any AI or ML technologies used in the processing of personal data and regularly reviews such systems to ensure ongoing compliance with global data protection standards.

Machine learning

Machine Learning (ML) is used to support internal processes such as project management, data analysis, communications, system security, anti-money laundering and fraud prevention. These technologies may be used, for example, to extract necessary information from documents submitted for identity verification (KYC), Anti-Money Laundering (AML), fraud detection, and transaction monitoring.

When photos and selfies are uploaded during the identity verification process, they are analyzed to confirm whether the individual registering matches the person shown in the provided identification. This technology scans images, converts them into digital templates, and compares them against each other and a database of images to determine a match.

We have developed machine learning models to support regulatory compliance by identifying potential transactional fraud. This analysis helps us provide requested services while meeting legal obligations related to fraud prevention, money laundering, and terrorism financing. The process involves analyzing transactional data, assigning values to specific indicators, and processing these values through a machine learning model to assess the likelihood of fraudulent activity.

Profiling and Automated Decision-making

When expressly agreed, we provide you with tailored information regarding our products and Services. We undertake data analysis in order to target appropriate communications and advertisements to you including invitations to exclusive client events that we think you may be interested in as well as recommending products and services that we think might be suitable for you.

In some cases, we use automated decision-making and profiling if it is authorized by legislation and necessary for the performance of a contract. For example, the automated authorization for remittance services. The legal basis to proceed with the profiling and the automated decision-making is legitimate interest.

We also make automated decisions in processes such as transaction monitoring in order to counter fraud in compliance with the legal requirements related to prevention of money laundering terrorist financing and financial services. Depending on your residence, you may have a right to request not to be subject to fully automated decision-making, including profiling, if such decision-making has legal effects or similarly significantly affects you. This right may not apply if the decision-making is necessary in order to enter into or to fulfil an agreement with you if the decision-making is permitted under applicable data protection laws or we have received your explicit consent.

Chatbot

Our services may include a chatbot functionality. This service records the conversations not only for quality assurance purposes but also to ensure compliance with our regulatory obligations.

In some cases, the chatbot feature is supported by an AI system. This service does not reuse your data nor learn from the data you post. This service is used to provide answers directly extracted from our systems.

Marketing Communications Based on Soft Opt-In and Consent

You may receive marketing communications from us through two different mechanisms:

1. Based on Your Consent (Regular Opt-In)

You will receive marketing messages if you have **explicitly given us permission** to use your Personal Data for that purpose. This occurs, for example, when:

- You opt in during registration; or
- You update your preferences in your profile settings.

With your consent, we provide tailored information about our products and services. We use data analysis to offer targeted communications, advertisements, and invitations to exclusive events, along with product and service recommendations that may interest you. You may withdraw your consent at any time.

2. Based on a Legitimate Interest (Soft Opt-In)

Where allowed by local law, you may also receive marketing communications if:

- You have a contractual relationship with us (e.g., you are actively using our Services); and
- You have not specifically opted out.

This applies only to products or services that are **similar to those you have used before**, and you will always be informed during registration and use of our Services that your Personal Data may be used for this purpose.

How to Opt Out or Withdraw Consent

You can stop receiving marketing communications at any time. If you do so, we will remove you from our marketing list and you will no longer receive promotional updates. You may also opt back in later if you wish.

You can withdraw your consent or opt out using any of the following:

- By updating your preferences in your profile;
- By clicking the **opt-out link** included in our communications;
- By contacting us at **dpo@euronetworldwide.com**.

If you have any additional questions or if you wish to **start receiving marketing communications**, please contact **dpo@euronetworldwide.com**.

Third Party Advertisement

Third-party advertisers provide advertisements that are displayed on our website, our App, or elsewhere in our Services. Third-party advertisers don't have access to any of the information our customers have given us directly. Typically, advertisers rely on cookies or some other web/app-based mechanism to assess which advertisements may be interesting to you.

We do not place “Targeting Cookies” or enable “Targeting” on your system without your consent, where required by law.

If you have provided your consent by accepting Targeting Cookies on the Website or enabled Targeting on the App, we may use third parties to do so (remarketing and Similar Audience features). With your consent, we may share your Personal Data with third parties for such marketing purposes. You can opt-out of advertising by modifying your cookies settings.

Third parties are not bound by our Privacy Notice. To understand the privacy practices of a third-party, you should visit the third-party website and review their privacy policy. You can find all the third parties that may use Cookies for targeting in our Cookie Policy.

Captcha and Bot Protection Tools

To protect our website and forms from spam, abuse, and automated misuse, we use CAPTCHA technologies. These tools analyze user behavior to distinguish human users from bots.

Where applicable, we may use non-intrusive CAPTCHA services to prevent fraud or abuse. These tools are designed to verify users without significantly affecting their experience. This processing is also based on our legitimate interest in securing our digital services.

Regional Privacy Notices

Notice to United States Residents for Financial Services

Applicability of Gramm-Leach-Bliley Act (GLBA)

This Notice informs U.S. consumers and customers (including former ones) about the federal Gramm-Leach-Bliley Act (“GLBA”) requirements. It concerns the collection, disclosure, and protection of “nonpublic personal information” (“NPI”).

For this Notice, NPI is personally identifiable information collected as a financial institution under the GLBA that is not publicly available. NPI may include any:

- Information provided by an individual when obtaining a financial product or service.
- Information obtained about an individual from transactions involving financial products or services.
- Information acquired about an individual in connection with providing a financial product or service, such as information from a consumer report or court record.

All disclosures of NPI are made as permitted by law. A “nonaffiliated third party” is any person except a financial institution’s affiliate or a person employed jointly by a financial institution and a company that is not the institution’s affiliate.

The **categories of information disclosed** and to whom under joint marketing/service provider exception of the Privacy Rule are listed [here](#)

If NPI may be disclosed to nonaffiliated third parties, and that disclosure does not fall within any of the exceptions of the Privacy Rule under the GLBA, consumers’ and customers’ have the right to opt out of these disclosures and an opt-out mechanism will be provided to the consumer or customer.

Notice of the information sharing among Euronet Group and it’s provided in accordance with the Fair Credit Reporting Act.

FACTS

WHAT DO WE DO WITH YOUR PERSONAL INFORMATION?

Why?

Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

What?	The types of personal information we collect, and share depend on the product or service you have with us. This information can include: Social Security Number and Identification Data Transactional Data and Financial and Employment information Location data and Behavioral and technical information When you are <i>no longer</i> our customer, we continue to share your information as described in this notice.	
How?	All financial companies need to share Consumer personal information to run their everyday business. In the section below, we list the reasons financial companies can share their consumer's personal information; the reasons We choose to share; and whether you can limit this sharing.	
Reasons we can share your personal formation	Do We Share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes— to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	Not applicable
For our affiliates' everyday business purposes— information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes— information about your creditworthiness	No	Not Applicable
For our affiliates to market to you	No	Not Applicable
For nonaffiliates to market to you	No	Not Applicable
Questions?	Call +18774431399 or go to https://help.riamoneytransfer.com/hc/en-us/requests/new	

Who we are	
Who is providing this notice?	Dandelion Payments, Inc.
What we do	

How do we protect your personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secure files and buildings. All personal information is stored in secure locations, protected by firewalls and other sophisticated security systems with restricted See security section of the global notice for further details or contact dpo@euronetworldwide.com
How do we collect my personal information?	We collect your personal information, for example, when you ▪ Send or Receive Money transfer Orders ▪ Register with an account ▪ Use or visit our online services ▪ Sign with our agents ▪ Use or request a service from us. We also collect your personal information from third parties' sources, government agencies, and consumer reporting agencies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. See the "Your Rights" section for more information
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and non-financial companies. ▪ We disclose your personal information with Euronet and Euronet Group affiliates for our everyday business purposes and compliance with group obligations.
Nonaffiliates	Companies not related by common ownership or control. They can be financial and non-financial companies. ▪ We disclose your personal information to perform compliance certification and fraud prevention and to enforce or apply our Terms and Conditions or any other agreement with you.
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you.
Other important information	

We comply with the rules issued to implement Executive Order 14117, restricting the exchange of Sensitive Personal Data with the identified countries of concern as defined under the Final Rule.

Universal Opt-Out Mechanism: We recognized an opt-out preference signal in a frictionless manner. The opt-out preference signal applies to your device, consumer, and/or offline sales, and grants you the right to opt-out of having your personal data shared for targeted advertising purposes. To implement an opt-out preference signal, please visit <https://globalprivacycontrol.org/> to learn how to download a supported browser or extension.

By providing your mobile number, you consent to receive SMS messages, including fraud alerts. When required, such messages will only be sent if you have previously consented. Message frequency may vary. Standard message and data rates may apply. You can opt out at any time by replying “STOP” or following the instructions in any message.

We will not share your number with third parties or affiliates for marketing or promotional purposes. We may share your number with subcontractors supporting service delivery, such as customer service. All text messaging consent data is excluded from such sharing.

California Residents

In accordance with the *California Consumer Privacy Act*, residents of California may exercise the following rights:

- Right to Know
- Right to Access
- Right to Correct Inaccuracies
- Right to Deletion
- Right to opt Out of Sale or Sharing of Personal Data for cross-contextual behavioral advertising purposes
- Right to limit Sensitive Personal Data use and disclosures to specifically permitted purposes.
- Right of No Retaliation Following opt-out or Exercise of other Rights

From the day we receive your request, we will respond to you within a maximum time of 45 days, unless an extension is requested. **Internal Appeals Process** If you receive notice from us that your Personal Data rights request has been refused, you may appeal the refusal within a reasonable period after receiving the notice by sending an email to dpo@euronetworldwide.com.

Our use of cookies or other tracking technologies may be considered a "sale" or "sharing" under applicable law. You may have the right to opt out of having your personal data shared for purposes of targeted advertising. We do not provide Services directly to children under 16, we do not knowingly sell or share personal information of consumers under 16 years of age.

In the prior 12 months, we may have shared the following categories of personal information: Identifiers such as contact information, internet and other electronic network activity information including behavioral and technical data.

In the prior 12 months, we may have shared your personal information to the following categories of third parties: Third-party service providers including advertisers or advertising networks and social media companies.

Texas Residents

If you have a complaint, first contact the consumer assistance division of Dandelion Payments, Inc. at [+18774431399](tel:+18774431399) if you still have an unresolved complaint regarding the company's activity, please direct your complaint to: Texas Department of Banking, 2601 North Lamar Boulevard, Austin, Texas 78705, 1-877-276-5554 (toll free), www.dob.texas.gov.

Notice to European (EEA) Residents

In accordance with the General Data Protection Regulation (GDPR) and in addition to the rights stated [above](#), all residents of the Economic European Area (EEA) may exercise the following rights:

- Right to Access
- Right to Correct Inaccuracies
- Right to Deletion
- Right to Restrict Processing
- Right to Data Portability
- Right to Object
- Rights related to Automated Individual Decision-Making

To exercise any of the rights listed above, you shall comply with the obligations set [above](#) in this Privacy Notice.

From the day we receive your request, we will respond to you within a maximum time of 30 days, unless an extension is requested.

While processing your Personal Data, we need to share your Personal Data according to the following:

Types of data	Purpose	Legal basis	Recipient
Identification data Financial data	To provide the Service on the RIA App	Legal obligation	Bank of Lithuania (Centrolink)
			PLAIS
			SERC

The Data Protection Authorities in the EEA are listed in this link, Europe (EEA): [Members | European Data Protection Board \(europa.eu\)](#)

Notice to UK Residents

In accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, all residents of the UK may exercise the following rights:

- Right to Access
- Right to Correct Inaccuracies
- Right to Deletion
- Right to Restrict Processing
- Right to Data Portability
- Right to Object
- Rights related to Automated Individual Decision-Making

To exercise any of the rights listed above, you shall comply with the obligations set [above](#) of this Privacy Notice, relating to sending our request to dpo@euronetworldwide.com and verification of your identity.

From the day we receive your request, we will respond to you within a maximum time of 30 days, unless an extension is requested.

To contact the Data Protection Authority, you can follow this link: [Information Commissioner Officer \(ICO\)](#)

Notice to Argentinian Residents

In accordance with the Personal Data Protection Act, Act No. 25.326 of 2000, you have the following rights, according to the definitions stated [above](#):

- Right to Access
- Right to Correct Inaccuracies
- Right to Rectification and update
- Right to Deletion

To exercise your Rights above or your right to revoke your consent, or if you have any questions or complaints regarding the processing of your Personal Data you may contact us at dpo@euronetworldwide.com.

You are also informed that you can limit the way we use or disclose your personal data for specific purposes, in accordance with your rights.

For request related to deleting or updating your Personal Data, we will respond with a maximum of 5 days.

For request regarding access to your Personal Data, we will respond within a maximum of 10 days. You are also informed that the Agency for Access to Public Information, in its capacity as the supervisory authority for the enforcement of Law No. 25,326, has the power to address complaints or violations related to the data protection laws. For more information on how to file a complaint, you may contact the supervisory authority directly: [Agencia de Acceso a la Información Pública](#)

Notice to Mexican Residents

In compliance with the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) and its Regulations, this Privacy Notice is provided to users and potential users in Mexico prior to collecting any personal data.

Personal Data is collected in line with the principles of legality, consent, information, quality, purpose, loyalty, proportionality, and responsibility.

Where biometric or sensitive data is processed, it will be based on your explicit consent.

You may exercise your ARCO rights (Access, Rectification, Cancellation, and Opposition), or revoke consent, by contacting: dpo@euronetworldwide.com. We will respond within 20 days, and implement any approved actions within 15 business days.

To contact the local Data protection authority follow this link: [Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales](#)

Notice to Chilean Residents

In accordance with Chile's Personal Data Protection Law, residents of Chile have the following rights (the "ARCO Rights"):

- Right to Access
- Right to Rectification
- Right to Deletion
- Right to Object
- Rights related to Automated Individual Decision-Making

Additionally, you have the right to withdraw your consent for the processing of your Personal Data at any time to the extent permitted by Law. To exercise your ARCO Rights, right to withdraw consent, or to ask any questions or submit complaints regarding the processing of your Personal Data, you may contact us at dpo@euronetworldwide.com.

Please be informed that options are available to limit the way we use or disclose your Personal Information for specific processing purposes.

From the day we receive your request, we will respond to you within a maximum timeframe of 30 days unless an extension is necessary.

To contact the local Data protection authority, follow this link: [Consejo para la Transparencia](#)

Notice to Malaysian Residents

In accordance with the *Personal Data Protection Act 2010* (the "PDPA"), customers may provide us with their Personal Data for any of the purposes establish in the What Type of Personal Information do we Collect Section of this Privacy Notice. If we were to process your Personal Data for any additional purpose, we will previously inform you or ask for your express consent.

In accordance with the *Personal Data Protection Act 2010* (the "PDPA"), all Malayan residents may exercise the following rights:

- Right to Access

- Right to Correct Inaccuracies
- Right to Deletion
- Right to Restrict Processing
- Right to Data Portability
- Right to Object

From the day we receive your request, we will respond to you within a maximum time of 21 days.

In accordance with the terms of the PDPA, we have the right to charge a fee for the processing of any data access request.

To contact the local Data protection authority, follow this link [Department of Personal Data Protection](#)

Notice to New Zealand Residents

To all resident in New Zealand, the rights you may exercise regarding the processing of your Personal Data are the following:

- Right to Know
- Right to Access
- Right to Correct Inaccuracies
- Right to Deletion
- Right to Restrict Processing

To exercise any of the rights listed above, you shall comply with the obligations set out in this Privacy Notice, relating to sending our request to dpo@euronetworldwide.com and verification of your identity.

From the day we receive your request, we will respond to you in a maximum time of 20 days.

To contact the local Data protection authority, go to: [Office of the Privacy Commissioner](#)

Notice to Australian Residents

To all residents in Australia, the rights you may exercise regarding the processing of your Personal Data are the following:

- Right to Know

- Right to Access
- Right to Correct Inaccuracies
- Right to Deletion
- Right to Restrict Processing

You may also ask us to explain our data policies and practices according to the applicable law.

From the day we receive your request, we will respond to you within a maximum time of 30 days.

While processing your Personal Data, we need to share your Personal Data according to the following:

Types of data	Purpose	Legal basis	Recipient
Identification data	To provide identity matching Services that help verify and protect your identity	Consent	Australian Government - Department of Home Affairs

To contact the local Data protection authority, go to: [Office of the Australian Information Commissioner](#)

Notice to Indian Residents

In accordance with the Indian Digital Personal Data Protection Act 2023, the Information Technology Act 2000 and the Information Technology Rules, all Indian residents may exercise the following rights:

- Right to Access
- Right to Correct Inaccuracies
- Right to Deletion
- Right to Restrict Processing
- Right to Data Portability
- Right to Object
- Rights related to Automated Individual Decision-Making

From the day we receive your request, we will respond to you within a maximum time of 30 days.

To contact the local Data protection authority, go to: [Department of Electronics and Information Technology](#)

Notice to Canadian Residents

To all residents in Canada, the rights you may exercise regarding the processing of your Personal Data are the following:

- Right to Know
- Right to Access
- Right to Correct Inaccuracies

From the day we receive your request, we will respond to you within a maximum of 30 days.

To contact the local Data protection authority, go to: [Office of the Privacy Commissioner of Canada](#)

Notice to Colombian Residents

In cases where required to fulfill our service obligations, we may lawfully conduct checks on criminal and judicial records to prevent money laundering, terrorist financing, and related offenses.

In accordance with Colombia's Statutory Law 1581 of 2012 and Decree 1377 of 2013, which govern personal data protection, Colombian residents have the right to Access, Update, Rectify, and Delete their data. To exercise these rights, revoke consent, or raise questions or complaints regarding the processing of your Personal Data, please contact us at: dpo@euronetworldwide.com , following the instructions provided in the “Your Rights” section above.

Upon receiving a request for information, we will respond within a maximum of 15 business days from the day following receipt of the request. For requests concerning claims, we will respond within a maximum of 23 business days from the day following receipt.

To contact the local Data protection authority: [Superintendencia de Industria y Comercio](#)

Notice to Senegal Residents

When you register with our App to use the Wallet service, we will collect personal data including your full name, email address, and phone number. The processing of this data is

based on our legitimate interest in correctly providing the service and ensuring the proper operation and continuous development of the App.

Beneficiaries receiving funds through our service may be contacted via SMS to notify them of the availability of such funds in the App. The legal basis for this communication is the provision of payment services under the PSD2 framework, which establishes legitimate interest of the data controller or a third party in fulfilling the contract with the payment service user.

In accordance with Law No 2008-12 of January 2008 and in addition to the rights stated [above](#), all residents of Senegal may exercise the following rights:

- Right to Access
- Right to Rectification
- Right to Deletion
- Right to Opposition
- Right to Limitation

From the day we receive your request, we will respond to you within a maximum time of 30 days, unless an extension is requested.

To contact the local Data protection authority: [Accueil - CDP](#)

Notice to Japanese Residents

In accordance with the Act on the Protection of Personal Information (APPI), the rights you may exercise regarding the processing of your Personal Data are the following:

- Right to Be Informed
- Right to Access
- Right to Correction
- Right to Deletion / Cessation of Use
- Right to Object to Third-Party Provision
- Right to Access Records of Third-Party Transfers
- Right to File a Complaint

From the day we receive your request, we will respond to you within a maximum of 30 days unless an extension is necessary.

To contact the local Data protection authority: [Personal Information Protection Commission \("PPC"\)](#)

Notice to Panama Residents

In accordance with Law No. 81 of 2019 and Executive Decree No. 285 of 2021, we inform you that certain additional requirements apply to the processing of personal data in Panama. These include the obligation to ensure that all notices provided to data subjects prior to the collection of their data include the disclosures required under Article 14 of the aforementioned Decree, and that consent, where applicable, is documented in a verifiable manner, including through technological means that ensure its traceability.

We also maintain an internal register of personal data transfers to third parties in accordance with applicable sectoral regulations. If you are a customer of remittance services or other regulated financial products, your information may be processed under the applicable legal exceptions provided for in Panamanian banking legislation.

The [National Authority of Transparency and Access to Information \(ANTAI\)](#) is the competent authority for any claims related to personal data protection in Panama.

Notice to Thailand Residents

In accordance with the Personal Data Protection Act B.E. 2562 (2019) ("PDPA"), residents of Thailand have the following rights regarding the processing of their Personal Data:

- **Right to Access** – You may request access to your Personal Data and obtain a copy.
- **Right to Rectification** – You may request correction of inaccurate or incomplete Personal Data.
- **Right to Erasure** – You may request deletion of your Personal Data under certain conditions.
- **Right to Restrict Processing** – You may request restriction of the use of your Personal Data.
- **Right to Object** – You may object to the processing of your Personal Data for specific purposes.
- **Right to Data Portability** – You may request to receive your Personal Data in a structured format or transfer it to another data controller.
- **Right to Withdraw Consent** – You may withdraw your consent at any time, unless restricted by law or contract.

- **Right to Lodge a Complaint** – You may file a complaint with the Office of the Personal Data Protection Committee (PDPC) if you believe your rights have been violated.

To exercise any of these rights, please contact us at dpo@euronetworldwide.com. We will respond to your request within 30 days, unless an extension is required.

If you wish to contact the local Data Protection Authority, you may reach the Office of the Personal Data Protection Committee (PDPC) via <https://www.pdpc.go.th>.

Notice to Puerto Rico residents

In accordance with the applicable federal laws of the United States, including the Gramm-Leach-Bliley Act (GLBA), and the Puerto Rico Personal Information Protection Act (Act No. 111-2005, as amended), we inform you of the following regarding the processing of your Personal Data:

Right of Access and Correction: You may request access to the personal information we maintain about you and request correction if it is inaccurate.

Restriction of Processing and Deletion: You may request the restriction of processing or deletion of your Personal Data in cases permitted by applicable law, unless we are required to retain such data due to contractual or regulatory obligations.

Security Breach Notification: In the event of a security breach that compromises your Personal Data, we will comply with the notification obligations established by Act No. 111-2005 and other applicable laws.

To exercise your rights, revoke your consent, or submit any inquiries or complaints related to the processing of your Personal Data, you may contact us at dpo@euronetworldwide.com, following the instructions set out in Section 10 of this Privacy Notice.

Please note that, as a financial institution, we are subject to legal obligations under U.S. federal regulations and the supervision of the [**Office of the Commissioner of Financial Institutions \(OCIF\)**](#) of Puerto Rico, which may require the retention and processing of certain Personal Data even if you request its deletion.

Other countries where we operate

Philippines

The [National Privacy Commission](#) is the competent authority for any claims related to personal data protection in Philippines

Brazil

The [Autoridade Nacional de Proteção de Dados](#) is the competent authority for any claims related to personal data protection in Philippines

South Africa

The [South Africa Information Regulator](#) is the competent authority for any claims related to personal data protection in Philippines

Our companies

The controller is RIA represented by the companies below, depending on country and service:

Currency Exchange Services

Country	Company to contact. (controller)	Contact details
Italy	Ria Italia S.r.l.	Via Francesco Benaglia, n. 13. 2°, Piano, Roma, 00153
Switzerland	Ria Financial Services GmbH	Langstrasse 192, 8005 Zürich
France	Ria France S.A.S	1-3 Rue du 19 Mars, Gennevilliers, 1962 92230, France
Belgium	Ria Envia Financial Services Belgium SRL	Rue Royale 153, 7ème étage, Saint-Josse-ten-Noode, 1210, Belgium
Germany	Ria Deutschland GmbH	Philipp-Johnson Haus, Suite 1.3, Friedrichstraße 200, Berlin, 10117, Germany
Sweden	Ria Financial Services Sweden AB	Armégatan 40, 5 tr 171 71 SOLNA. Stockholms län, Stockholm kommun, Sweden
Norway	Ria Financial Services Norway AS	Schweigaards gate 6, 0185, Norway
Denmark	Ria Financial Services Denmark ApS	Nørre Voldgade 21. 1358 København K, Copenhagen, 1358, Denmark
UK	Euronet Payment Services Ltd.	Part 7th Floor, North Block, 55 Baker Street, London, United Kingdom, W1U 7EU
Spain	Ria Payment Institution EP SAU	Calle Cantabria 2, Planta 2 Alcobendas 28108 Madrid España
Poland	Euronet Polska Sp. zo.o	Ul. Inflancka 4c, 00-189 Warsaw, Poland
Malaysia	IME M SDN BHD	Level 11, Menara TH 1 Sentral, Jalan Rakyat, Kuala Lumpur Sentral, 50470 Kuala Lumpur, Malaysia
Netherlands	Xe Europe B.v.	Rozengracht 12-1, 1016 NB Amsterdam, Netherlands
Canada	Gescoro, Inc.	5065 R. Saint-Denis Montréal, QC H2J 2L9, Montreal (Québec), Canada

You can always submit a request to our Data Protection Officer by sending an email to the following address: dpo@euronetworldwide.com.

Money Transfer Services

Country	Company to contact. (controller)	Contact details
United Kingdom	Euronet Payment Services Ltd.	Part 7 th Floor, North Block, 55 Baker Street, London, United Kingdom, W1U 7EU
Europe (Digital and mobile)	Ria Lithuania UAB	Ukmergės g. 126, Vilnius, LT-08100, Lithuania
Europe	Ria Payment Institution EP SAU	Calle Cantabria 2, Planta 2 Alcobendas 28120 Madrid España
Switzerland	Ria Financial Services GmbH	Langstrasse 192. Zürich, 8005, Switzerland
United States	Dandelion Payments, Inc.	7000 Village Drive, Suite 200, Buena Park, 90621-2232, United States
Puerto Rico	Ria Financial Services Puerto Rico, Inc.	2104 Borinquen Avenue Santurce, San Juan, 00915, Puerto Rico
Canada	Ria Telecommunications of Canada Inc	5065 R. Saint-Denis Montréal, QC H2J 2L9, Montreal (Québec), Canada
México	Ria México Payment Solutions, S. de R.L. de C.V.	Av. Anillo Vial Fray Junípero Serra 21260 PAD 07 PB Loc B Jurica Queretaro, Queretaro 76147. Mexico, 03100, Mexico
Chile	Ria Chile Servicios Financieros SPA	Avenida Libertador Bernardo O'Higgins. N° 1449, Torre 4, ofc 1502. Santiago de Chile, Chile
Argentina	Euronet Payment Services Ltd Sucursal Argentina	Av. Santa Fe 1752 N° 1 A, Buenos Aires, C1060ABQ, Argentina.
Malaysia	IME (M) Sdn Bhd Pte.Ltd	Level 11, Menara TH 1 Sentral, Jalan Rakyat, 50470 Kuala Lumpur, Malaysia.
Singapore	Ria Financial Services Singapore Pte. Ltd.	152 Beach Road, The Gateway (East) 9-01/02, Singapore, 189721.
Philippines	Ria Money Transfer, Inc.	8F Zuellig Building, Makati Ave. cor. Paseo de Roxas & Sta Potenciana Str. Makati City, 1225, Philippines
Australia	Ria Financial Services Australia Pty Ltd	Level 1, 75 Castlereagh Street, Sydney, NSW 2000, Australia
New Zealand	Ria Financial Services New Zealand Ltd	32 Mahuhu Crescent Level 4, Auckland, 1010, New Zealand
Japan	Unidos Co Ltd.	Stairs Building, 2F, 2-4-8 Hyakunincho, Shinjuku-ku, Tokyo 169-0073, Japan
India	Ria Money Transfer Services Pvt. Ltd	I-Think Techno Campus, Office N° 1, Wing A, 8th Floor Off Pokhran Road N° 2, Behind Yantra Park – TCS, Eastern Express Highway, Thane West. Maharashtra, 400 607, India
Colombia	Ria Money Transfer Colombia S.A.	Calle 127 No. 70G-68 Oficina 412 Bogotá D.C., Colombia
Panama	Ria Money Transfer Panamá S. de R.L.	Albrook Gran Terminal de Transporte - Local L-08, Ciudad de Panamá, Panamá

Contact Euronet Privacy

For queries, suggestions, or complaints, please contact our Privacy department directly.

- Email: dpo@euronetworldwide.com
- Postal mail: DPO, Calle Cantabria 2, 2-A Alcobendas Madrid, Spain