PRIVACY NOTICE

Updated: 15 November 2024

Introduction

This notice talks about your privacy and applies across all websites that we own and operate and all services we provide, including our online and mobile services, and any other apps or services we may offer (for example, events or training).

When we say 'personal data' we mean identifiable information about you, like your name, email, address, telephone number, bank account details, payment information, support queries, community comments and so on. If you can't be identified (for example, when personal data has been aggregated and anonymised) then this notice doesn't apply.

We may need to update this notice from time to time. Where a change is significant, we'll make sure we let you know - usually by sending you an email.

Who are 'we'?

When we refer to 'we' (or 'our' or 'us'), that means Remit One Limited and all its wholly owned subsidiaries. Our headquarters are in the UK but we operate and have offices all over the world. Please visit our contact us page for address details.

We provide a web-based remittance management platform for money transfer operators. To find out more about what we do, please visit our what we offer page.

For European Union data protection purposes, when we act as a controller in relation to your personal data, Remit One Limited (company number 06446656) is our representative in the European Union.

Our principles of data protection

Our approach to data protection is built around four key principles. They're at the heart of everything we do relating to personal data.

Transparency: We take a human approach to how we process personal data by being open, honest and transparent.

Enablement: We enable connections and efficient use of personal data to empower productivity and growth.

Security: We champion industry leading approaches to securing the personal data entrusted to us.

Stewardship: We accept the responsibility that comes with processing personal data.

How we collect your data

When you visit our websites or use our services, we collect personal data. The ways we collect it can be broadly categorised into the following:

Information you provide to us directly
When you visit or use some parts of our websites and/or services we might ask you to provide personal data to us. For example, we ask for your contact information when you sign up for services, respond to a job application or an email offer, participate in community forums, join us on social media, take part in training and events, contact us with questions or request support. If you don't want to provide us with personal data, you don't have to, but it might mean you can't use some parts of our websites or services.

Information we collect automatically
We collect some information about you automatically when you visit our websites or use our services, like your IP address and device type. We also collect information when you navigate through our websites and services, including what pages you looked at and what links you clicked on. This information is useful for us as it helps us get a better understanding of how you're using our websites and services so that we can continue to provide the best experience possible (e.g., by personalising the content you see).

Some of this information is collected using cookies and similar tracking technologies. If you want to find out more about the types of cookies we use, why, and how you can control them, take a look at our cookie notice.

Information we get from third parties
The majority of information we collect, we collect directly from you. Sometimes we might collect personal data about you from other sources, such as publicly available materials or trusted third parties like our marketing and research partners. We use this information to supplement the personal data we already hold about you, in order to better inform, personalise and improve our services, and to validate the personal data you provide.

Where we collect personal data, we'll only process it:

- to perform a contract with you, or
- where we have legitimate interests to process the personal data and they're not overridden by your rights, or
- in accordance with a legal obligation, or
- where we have your consent.

If we don't collect your personal data, we may be unable to provide you with all our services, and some functions and features on our websites may not be available to you.

If you're someone who doesn't have a relationship with us, but believe that a Remit One subscriber has entered your personal data into our websites or services, you'll need to contact that Remit One subscriber for any questions you have about your personal data (including where you want to access, correct, amend, or request that the user delete, your personal data).

How we use your data

First and foremost, we use your personal data to operate our websites and provide you with any services you've requested, and to manage our relationship with you. We also use your personal data for other purposes, which may include the following:

To communicate with you
This may include:

- providing you with information you've requested from us (like training or education materials) or information we are required to send to you
- operational communications, like changes to our websites and services, security updates, or assistance with using our websites and services
- marketing communications (about Remit One or another product or service we think you might be interested in) in accordance with your marketing preferences
- asking you for feedback or to take part in any research we are conducting (which we may engage a third party to assist with).

To support you
This may include assisting with the resolution of technical support issues or other issues relating to the websites or services, whether by email, or otherwise.

To enhance our websites and services and develop new ones
For example, by tracking and monitoring your use of websites and services so we can keep improving, or by carrying out technical analysis of our websites and services so that we can optimise your user experience and provide you with more efficient tools.

To protect
So that we can detect and prevent any fraudulent or malicious activity, and make sure that everyone is using our websites and services fairly and in accordance with our terms of use.

To market to you
In addition to sending you marketing communications, we may also use your personal data to display targeted advertising to you online – through our own websites and services or through third party websites and their platforms.

To analyse, aggregate and report
We may use the personal data we collect about you and other users of our websites and services (whether obtained directly or from third parties) to produce aggregated and anonymised analytics and reports, which we may share publicly or with third parties.

How we can share your data

There will be times when we need to share your personal data with third parties. We will only disclose your personal data to:

- other companies in the Remit One group of companies

- third party service providers and partners who assist and enable us to use the personal data to, for example, support delivery of or provide functionality on the website or services, or to market or promote our goods and services to you

- regulators, law enforcement bodies, government agencies, courts or other third parties where we think it's necessary to comply with applicable laws or regulations, or to exercise, establish or defend our legal rights. Where possible and appropriate, we will notify you of this type of disclosure

- an actual or potential buyer (and its agents and advisers) in connection with an actual or proposed purchase, merger or acquisition of any part of our business

- other people where we have your consent.

International data transfers

When we share data, it may be transferred to, and processed in, countries other than the country you live in - such as to the United Kingdom, where our data hosting provider's servers are located. These countries may have laws different to what you're used to. Rest assured, where we disclose personal data to a third party in another country, we put safeguards in place to ensure your personal data remains protected.

For individuals in the European Economic Area (**EEA**), this means that your data may be transferred outside of the EEA. Where your personal data is transferred outside the EEA, it will only be transferred to countries that have been identified as providing adequate protection for EEA data, or to a third party where we have approved transfer mechanisms in place to protect your personal data – i.e., by entering into the European Commission's Standard Contractual Clauses, or by ensuring the entity is Privacy Shield certified (for transfers to US-based third parties). For further information, please contact us using the details set out in the How to contact us section below.

Security

Security is a priority for us when it comes to your personal data. We're committed to protecting your personal data and have appropriate technical and organisational measures in place to make sure that happens. For more information about security, check out Remit One's security notice.

Retention

The length of time we keep your personal data depends on what it is and whether we have an ongoing business need to retain it (for example, to provide you with a service you've requested or to comply with applicable legal, tax or accounting requirements).

We'll retain your personal data for as long as we have a relationship with you and for a period of time afterwards where we have an ongoing business need to retain it, in accordance with our data retention policies and practices. Following that period, we'll make sure it's deleted or anonymised.

Your rights

It's your personal data and you have certain rights relating to it. When it comes to marketing communications, you can ask us not to send you these at any time - just follow the unsubscribe instructions contained in the marketing communication, or send your request to privacy@remitone.com.

You also have rights to:

- know what personal data we hold about you, and to make sure it's correct and up to date

- request a copy of your personal data, or ask us to restrict processing your personal data or delete it
- object to our continued processing of your personal data
- You can exercise these rights at any time by sending an email to privacy@remitone.com.

If you're not happy with how we are processing your personal data, please let us know by sending an email to privacy@remitone.com. We will review and investigate your complaint, and try to get back to you within a reasonable time frame. You can also complain to your local data protection authority. They will be able to advise you how to submit a complaint.

How to contact us

We're always keen to hear from you. If you're curious about what personal data we hold about you or you have a question or feedback for us on this notice, our websites or services, please get in touch.

As a technology company, we prefer to communicate with you by email - this ensures that you're put in contact with the right person, in the right location, and in accordance with any regulatory time frames.

Our email is privacy@remitone.com.

COOKIE NOTICE

Updated: 15 November 2024

Introduction

This notice talks about the cookies and similar tracking technologies that we use and applies across the websites we operate and all services we provide, including our online and mobile services, and any other apps or services we provide to you.

We may need to update this notice from time to time. Where a change is significant, we'll make sure we let you know - usually by sending you an email.

What cookies and tracking technologies do we use?

A cookie is a small text file that's placed on your computer or mobile device when you visit one of our websites. We, and some of our affiliates and third-party service providers, may use a few different types of cookies. Some are persistent cookies (cookies that remain on your hard drive for an extended period of time) and some are session ID cookies (cookies that expire when you close your browser).

We also use other tracking technologies like web beacons (sometimes called "tracking beacons" or "clear gifs") and local storage. These are tiny graphics files that contain a unique identifier that enable us to recognise when someone has visited our websites or opened an email that we have sent them.

Why do we use cookies and tracking technologies?

They help us to do awesome things like operate our websites and services, enhance and customise your experience across our websites and services, perform analytics and deliver advertising and marketing that's relevant to you.

There are also cookies set by third parties across our websites and services. Third party cookies enable third party features or functionality to be provided on or through our websites and services, such as advertising, interactive content and analytics. They also enable us to use advertising networks to manage our advertising on other websites.

Remit One cookies

Below is a list of cookies that we may use on our websites and services. The types of cookies we may use are always changing. Check back regularly to make sure you stay up to date. If you think we've missed a cookie, please let us know.

Essential Cookies
These cookies are necessary for the functionality of the websites and services. These cookies can be disabled in your browser but may prevent certain parts of the websites and services from functioning.

Analytics Cookies
These cookies help us to determine the source and amount of traffic to the websites and services and help us to better understand how our visitors use the websites and services. If you choose to disable these cookies, it will impact our ability to measure the performance of the website and services.

Functionality Cookies
These cookies help us to enhance the functionality of our websites and services, including through the use of customisation or personalisation. These cookies may be set by third parties. Disabling these cookies may prevent certain parts of the websites and services from functioning.

Advertising or Targeting Cookies
These cookies may be set by third parties to facilitate the delivery of targeted advertising, including through the delivery of interest-based advertising, and helping us measure the effectiveness of our campaigns. If you disable these cookies, you may receive less relevant or targeted advertising.

How can you control cookies?

You can accept or reject cookies by amending your web browser controls. Because they're important, our websites and services might not work like they're supposed to, and in some cases, might not work at all, if you decide to reject our cookies.

Most advertising networks also offer you the option to opt out of targeted advertising. For more info, visit http://www.aboutads.info/choices/ or http://www.youronlinechoices.com.

You can manage your cookie settings by following your browser's instructions. Here are some links that might be of assistance:

Google Chrome
https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=en

Microsoft Internet Explorer
https://support.microsoft.com/en-nz/help/17442/windows-internet-explorer-delete-manage-cookies

Mozilla Firefox
https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences

Safari
https://support.apple.com/en-nz/guide/safari/manage-cookies-and-website-data-sfri11471/mac

SECURITY NOTICE

Updated: 15 November 2024

Introduction

This notice talks about the steps we take to keep our systems and your data secure.

We may need to update this notice from time to time. Where a change is significant, we'll make sure we let you know - usually by sending you an email.

Protecting Your data

We're committed to the security of our customers' data and provide multiple layers of protection for the personal and financial information you trust to Remit One.

You control access

As a Remit One customer you have the flexibility to invite unlimited users into your system to collaborate on your data, and the person that holds the subscription has control over who has access and what they are able to do. Our customer support team will not access your information unless you invite them to help. Please see our privacy notice for further information.

User authentication

We provide standard access to the Remit One software through a login and password. In addition, we offer the option of using two-step authentication. This provides a second level of security for your Remit One system. It means You're also asked to enter a unique one-time code generated by a separate authenticator system. We recommend you use two-step authentication as it reduces the risk of your Remit One system being accessed if your password is compromised.

Data encryption

We encrypt all data that goes between you and the Remit One system using industry-standard TLS (Transport Layer Security), protecting your personal and financial data. Part of your data is also encrypted at rest when it is stored on our servers, and encrypted when we transfer it between data centres for backup and replication.

Network protection

Remit One takes a 'defence in depth' approach to protecting our systems and your data. Multiple layers of security controls protect access to and within our environment, including firewalls, intrusion protection systems and network segregation. Remit One's security services are configured, monitored and maintained according to industry best practices.

Secure data centres

Remit One's servers are located within enterprise-grade hosting facilities that employ robust physical security controls to prevent physical access to the servers they house. These controls include 24/7/365 monitoring and surveillance, on-site security staff and regular ongoing security audits. Remit One maintains multiple geographically separated data replicas and hosting environments to minimise the risk of data loss or outages.

Security monitoring

Remit One's Security team continuously monitors security systems, event logs, notifications and alerts from all systems to identify and manage threats.

Best in class availability

Remit One delivers best-in-class availability. We use multiple redundancy technologies for our infrastructure. These ensure that if any component fails, Remit One systems will keep on running - with little disruption to your service.

Built to perform at scale

Remit One systems have been designed to grow with your business. Our high-performance servers, networks and infrastructure ensure we can deliver quality service to you and our thousands of other users.

Disaster recovery and readiness

Remit One performs real-time data replication between our geographically diverse, protected facilities, to ensure your data is available and safely stored. This means that should even an unlikely event occur, such as an entire hosting facility failure, we can switch over to a backup site to keep Remit One systems and your business running. We transmit data securely, across encrypted links.

Constant updates and innovation

We're constantly enhancing Remit One's systems, delivering new features and performance improvements. Updates are generally delivered quarterly.

Your online safety

We design security into Remit One systems from the ground up. However, there can be risks to working and playing online. Whether you're shopping, banking, doing your accounts, or simply checking your email, cyber criminals and scammers are always looking for ways to steal money or sensitive information. There are precautions you can take to reduce the risks and help keep You safe from harm online. See below for information about how to identify and deal with scams and malicious 'phishing' emails.

Phishing and malicious emails

A phishing email is a favoured way for cyber criminals to get access to your sensitive information, such as your usernames and passwords, credit card details, bank account numbers, etc. This kind of email may look as if it has come from a trustworthy source, but will attempt to trick you into:

- clicking on a link that will infect your computer with malicious software;
- following a link to a fake (but convincing looking) website that will steal your login details;
- opening an attachment that will infect your computer.

Once you are hooked, the cyber-criminal may be able to steal or extort money from you, or gather sensitive personal or business information that they can use for other attacks. However, you can protect yourself and your business by being aware of these scams, and by knowing what to look for that may help you identify a malicious email, for example:

- incorrect spelling or grammar: legitimate organisations don't always get it 100% right, but be suspicious of emails with basic errors;
- the actual linked URL is different from the one displayed – hover your mouse over any links in an email (DON'T CLICK) to see if the actual URL is different;
- the email asks for personal information that they should already have, or information that isn't relevant to your business with them;
- the email calls for urgent action, for example, "your bank account will be closed if you don't respond right away"; if you are not sure and want to check, then go directly to the bank's website via the URL you would normally use, or phone them, but don't click on the link in the email;
- the email says you've won a competition you didn't enter, have a parcel waiting that you didn't order, or promises huge rewards for your help - on the internet, if it sounds too good to be true then it probably isn't true;
- there are changes to how information is usually presented, for example an email is addressed to "Dear Sirs" or "Hello" instead of to you by name, the sending email address looks different or complex, or the content is not what you would usually expect.

These are just a few of the things to watch out for. There's a lot more information and tips available on the web. But even if there's nothing specific You can point to, the email may just not "feel" right. Trust your instincts, and don't get hooked.

If you suspect you've received a phishing or malicious email, and it says it's from Remit One or uses Remit One's logo, do not click on anything in the email - please report it by forwarding the email to phishing@remitone.com.

Try to avoid a phishing attack by following these rules

If You receive a suspicious email make sure You:

1. DO NOT CLICK on any link or attachment contained in the email.

2. DO NOT REPLY to the email.

3. Report the email by forwarding it to phishing@remitone.com if it is Remit One branded.

4. Delete the email.

5. Update your anti-malware (anti-virus, anti-spyware) and run a full scan on your computer.