

ZING

Privacy Notice (UK)

For peace of mind





[Your personal data](#)

[How we'll use your personal data](#)

[Who we share your personal data with](#)

[Other important information](#)

[Your rights](#)

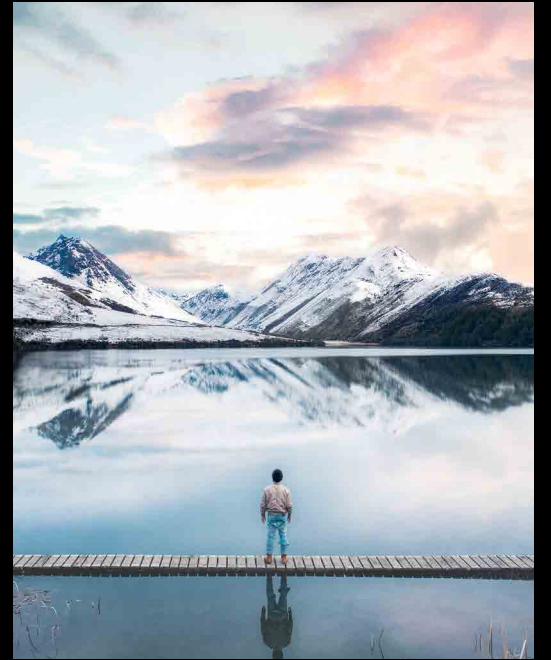
Contents



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

None of the
borders,
all of the
Zing





[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

Welcome

We just want to let you know that we'll collect some information about you. We use this information to deliver our services to you and comply with the law. We also use it for other things, which we think help you and us. Most organisations do this. We've put this notice together to explain what we do in more detail. Got questions? Reach out to us using the Zing [app](#) messaging function or emailing us at privacy@zing.me.

When we talk about "we", "our" or "us" in this Privacy Notice we mean MP Payments UK Limited.





[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

How we collect your information

We collect information about you from a range of places. Sometimes, you share information with us when you:

- call or message us;
- visit our website;
- use our app; or
- join our mailing list.

We may also collect information about you to:

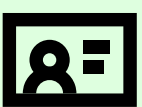
- prevent fraud or crime; and
- comply with the law.

We may collect this information using technology (such as cookies or pixels) or by asking third parties.

You can read more about [how we collect your information here.](#) 

What we collect

We may collect:



Personal details and contact data (such as your name or date of birth)



Identity data (such as your Photo ID or passport)



Financial and relationship data (such as information about your Zing account)



Regulatory and investigations data (such as anti-money laundering checks)

Some of the data we collect about you may be sensitive data. 

Find out more about [what we collect here.](#) 



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)


How we use this information

We may use this information:

- to verify your identity;
- when carrying out background checks; and
- to prevent or detect crime.

We may also use it to:



- provide our products and services to you;
- for marketing and advertising; and
- business and administrative purposes.

More details about [what we use your information for can be found here.](#) 

Who we share your information with

We may share your information if it's lawful. For example, we may do this if we have a legitimate business reason for doing so.

This means that we may share your information with:

- people and companies that you pay, or who make payments to you;
- our group companies;
- our third party service providers;
- anyone you've agreed to us sharing, or have asked us to share, your personal data with;
- relevant public authorities;
- parties involved in disputes;
- parties in connection with a partial or full, potential or actual merger, acquisition or takeover;
- [social media platforms and third party advertisers;](#) 
- [fraud prevention agencies.](#) 

You can read more [about it here.](#) 



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

How long we'll keep your information

We'll only keep your information for as long as we need it. After that, we'll either delete it or change it so no one can tell it's about you.

You can read more [about it here](#). 

Transferring your personal data overseas

Sometimes, your information may be sent to or stored (including being accessed from) locations outside the United Kingdom. When this happens, we ensure:

- appropriate safeguards are in place; and
- the transfer is in line with applicable legal requirements.

You find out more details about [what happens to your data here](#). 

Our commitment to you

We're committed to protecting your personal data. We use a range of technical, physical and organisational measures to help keep your personal data safe. These include:

- secure authentication requirements;
- encryption; and
- other forms of security.


We also make sure our employees and third parties adopt appropriate security standards.

How we make decisions

We may use automated systems to help us make decisions, such as:

- fraud and money laundering checks; or
- assessing risks related to accounts.

These automated decisions aren't final. A human will usually investigate before any significant decision is made.

You can find more details about [automated decisions here](#). 



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

Your rights

We think carefully about how we use your information. We always aim to use it in a way that's fair to you. You might prefer us not to use it for some purposes.

You have a legal right to:

- ask us to provide you with copies of your personal information, make corrections or sometimes ask us to delete it;
- tell us you no longer consent to us processing your personal information;
- object to our processing of your information (in some circumstances) or ask us to limit it.

You can find out [more about your rights here.](#) 

We're not responsible for other websites

We have links to other websites on our own website. We don't own or operate these other websites. They have their own privacy notices. We don't accept any responsibility or liability for their:

- policies about any personal data; or
- collection or processing of any personal data.





[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

Who's responsible for your personal data?

MP Payments UK Limited is the controller of your personal data. This means that we make the decisions about what personal data we collect and how it is used. The address for MP Payments UK Limited is 8 Canada Square, London, E14 5 HQ.

Complaints

If you're unhappy with how we've handled your personal information then let us know. We'll try our best to sort things out. You can email your complaints to our Data Protection Officer at: DPO@zing.me.

You have a right to complain to the UK Information Commissioner's Office. You can do this by visiting ico.org.uk.

This Privacy Notice may be updated from time to time, and the most recent version can be found at <https://wearemp.com/pdfs/PrivacyPolicy.pdf>.

This notice was last updated in [Month YYYY].

Take your
money
global





[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data](#)



[Other important information](#)



[Your rights](#)



1. Your personal data

1.1 How do we collect your personal data?

We collect information about you from a range of places. Sometimes, you share information with us (either directly or via a third party acting on our behalf). For example, during the account management process or when you sign up to receive marketing. You must ensure that all information you share with us is correct and up to date. You'll tell us as soon as possible of any changes.

We may also collect information about you when:

- you interact with us and agree to share this information (where appropriate). For example, when you message us, visit our website, fill in our surveys, enter our competitions or promotions, share information on social media with us, or use our app.
- we have a duty to collect certain information to prevent financial crime and to comply with sanctions laws. We collect this from:
 - third parties such as fraud prevention agencies (see [Fraud and Money Laundering](#));
 - other HSBC companies; and
 - our screening services provider.



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data](#)



[Other important information](#)



[Your rights](#)

Information may be sourced from publicly accessible sources, such as Electoral Registers (either directly or indirectly). This includes political affiliations, sanctions, and unlawful or criminal activities such as terrorism. Our third party provider may also use publicly accessible sources to check your address if you have chosen to check it using databases during onboarding.

Cookies

Some of the information we collect automatically via our website and app is collected using cookies or similar technologies. These may track and record your interactions with the website or app in order to:

- keep you safe;
- help keep our services secure;
- help make your visit more personal; or
- to support our marketing.

For more information, please read our [Cookie Notice](#).

Pixels

We also use pixels or web beacons in our direct marketing emails.

These pixels track whether:

- our email was delivered and opened; and
- links within the email were clicked.

They also allow us to collect information about your device and internet connection. This includes your IP address, browser, email client type and other similar details.

We use this information to:

- measure the performance of our email campaigns;
- improve our communications; and
- send you more relevant information and marketing.



[Your personal data](#)

[How we'll use your personal data](#)

[Who we share your personal data](#)

[Other important information](#)

[Your rights](#)

1.2 What personal data do we collect about you?

If you've applied for a Zing account, then we may collect:



Personal Details and Contact Data

This includes your:

- name;
- gender;
- date of birth;
- residential address;
- email address; and
- telephone number.



Identity Data

This is information we use to identify you. This may include your:

- photo ID;
- passport information;
- national ID card;
- nationality;
- video selfie; and
- user login details for the Zing app.



Financial and Relationship Data

This is information about your finances and your relationship with us such as:

- information about your Zing account;
- any other products and services you hold with us;
- your payment history, transaction records and risk rating information; and
- information about your interactions with us (including any requests, complaints or disputes and advice we've given you).



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data](#)



[Other important information](#)



[Your rights](#)



Regulatory and Investigations data

This includes:

- due diligence checks, sanctions and anti-money laundering checks;
- detection of any suspicious or unusual activity and associated reporting. This includes details about people connected to you or relevant activities, and records about these things; and
- any other information we need to support our regulatory obligations.



Sensitive Data

Certain types of personal data are given special protections under data protection laws. This includes:

- special category data (such as religious or philosophical beliefs, biometric data where it's used for identification purposes and information about your physical or mental health); and
- information relating to criminal convictions and offences.

We may use these types of information:

- to verify your identity;
- when carrying out background checks; or
- to prevent or detect crime (including speaking with the relevant authorities where appropriate).

Connected Persons

We may process information about you when a family member or a person you have a business relationship applies for or holds an account with us. We carry out these checks for fraud and crime prevention purposes. This may include regulatory and investigations data and sensitive data.

Customer Contacts

We may process information when a person you know shares their phone contacts with us. E.g., email and phone number.



[Your personal data](#)

[How we'll use your personal data](#)

[Who we share your personal data with](#)

[Other important information](#)

[Your rights](#)



2. How we'll use your personal data

2.1 Legal basis

We'll only use your personal data if:

Reason	Explanation	Legal Basis
 The law makes us	We're legally required to collect this personal data. E.g., carrying out and keeping records of our anti-money laundering checks.	Contractual necessity
 You agree	You've told us we can use your personal data for a particular purpose.	Consent
 It's in the public interest	We believe it's in the public interest for us to do so. E.g., to help prevent or detect crime.	Public Interest
 We have a legitimate interest	We have a legitimate interest we need to pursue and your interests or fundamental rights and freedoms don't override these interests.	Legitimate Interest
 To exercise our legal rights	We need to establish, utilise or defend our legal rights.	Legal Rights



[Your personal data](#)

[How we'll use your personal data](#)

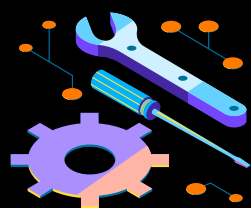
[Who we share your personal data with](#)

[Other important information](#)

[Your rights](#)

2.2 How we can use your personal data

We may use your personal data for the following reasons:



Providing our products and services

Reason for data collection	Legal basis for collecting data
<p>To verify your identity and to carry out background checks to:</p> <ul style="list-style-type: none"> prevent or detect crime, including fraud and financial crime; and comply with sanctions laws, including checking applications against certain fraud prevention and sanctions databases. <p>As part of our onboarding process, if you choose to share your location with us and the suppliers who help us provide this functionality, we can verify your home address without requiring separate proof of address.</p> <p>We may use the photo you share with us during other customer's onboarding to check they are not fraudulent or duplicating your account.</p>	<ul style="list-style-type: none"> Legal obligation Contractual obligations Legitimate interest in: <ul style="list-style-type: none"> preventing fraud and money laundering; confirming your identity in order to protect our business; and complying with our legal and regulatory obligations in an effective and efficient manner. Consent (if given) to use location services to verify your home address. <p>To the extent such information is 'special category' personal data, also:</p> <ul style="list-style-type: none"> Substantial public interest.
<p>To check product eligibility.</p> <p>This ensures that requirements are met and risk assessments are carried out to measure, detect and prevent the likelihood of financial, reputational, legal, compliance or customer risk.</p>	<ul style="list-style-type: none"> Legitimate interests in: <ul style="list-style-type: none"> managing our risk profile to protect our business; and complying with our legal and regulatory obligations in an effective and efficient manner.



[Your personal data](#)

[How we'll use your personal data](#)

[Who we share your personal data with](#)

[Other important information](#)

[Your rights](#)

Reason for data collection	Legal basis for collecting data
<p>To provide and manage our financial products and services in line with our contracts and applicable laws and regulations.</p> <p>Financial services include:</p> <ul style="list-style-type: none"> • moving money between wallets; and • making payments. 	<ul style="list-style-type: none"> • Legal obligation • Contractual obligation • Legitimate interest in: <ul style="list-style-type: none"> ◦ providing our customers with great products and services; and ◦ complying with our legal and regulatory obligations in an effective and efficient manner.
<p>To provide and manage the Zing app and our website, including:</p> <ul style="list-style-type: none"> • keeping them secure, allowing you to log in securely protecting against fraud and crime; • keeping our services running reliably, including checking for and resolving any issues, and ensuring it works on your device; and • trialling new designs and layouts to see which our customers prefer. 	<ul style="list-style-type: none"> • Legal obligation • Contractual obligation • Legitimate interest in: <ul style="list-style-type: none"> ◦ providing our customers with great products and services; ◦ keeping our customers and their information safe; ◦ preventing fraud and money laundering and confirming your identity in order to protect our business; and ◦ complying with our legal and regulatory obligations in an effective and efficient manner. • Consent (if given).
<p>To provide you with optional functionality, such as Contact Sync.</p> <p>Contact Sync is a service where you have agreed to connect your phone contacts to let us see whether your contacts are also Zing customers. This means you can make payments to them. We will regularly collect this information to make sure it stays up to date.</p> <p>You'll only see a contact's name if they have also switched on this feature. To make sure you pay the right person, you'll see their full name (as per their account). Your contacts will also be able to see your name and know you have a Zing account. You can turn this feature on and off via our app settings.</p>	<ul style="list-style-type: none"> • Consent (if given).



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

Reason for data collection	Legal basis for collecting data
<p>To manage our relationship with you, including:</p> <ul style="list-style-type: none"> • providing you with product and service updates; and • customer support. We may provide additional support for vulnerable customers. <p>Please note that we may record and monitor any communications with you (by whatever channel) and associated information such as the number you're calling from and information about your device or software.</p> <p>We may use this information to check your instructions, for training and quality control purposes, to assess, analyse and improve our products and services, to manage risk and to prevent and detect fraud or other crimes.</p>	<ul style="list-style-type: none"> • Contractual obligation • Legitimate interest in: <ul style="list-style-type: none"> ◦ providing our customers with great products and services; ◦ keeping our customers and their information safe; ◦ preventing fraud and money laundering, confirming your identity to protect our business and our customers, complying with applicable law; and ◦ complying with our legal and regulatory obligations in an effective and efficient manner. <p>To the extent such information is 'special category' personal data:</p> <ul style="list-style-type: none"> • Substantial public interest.
<p>To prevent and detect crime, including fraud, money laundering, and terrorist financing through:</p> <ul style="list-style-type: none"> • carrying out monitoring, mitigation and risk management, customer due diligence, and transaction screening and monitoring; • sharing information with law enforcement, relevant authorities and other third parties where permitted by law; and • taking steps to help prevent financial crime and to manage risk. 	<ul style="list-style-type: none"> • Legal obligation • Legitimate interest in: <ul style="list-style-type: none"> ◦ preventing fraud and money laundering in order to protect our business and our customers; ◦ complying with applicable laws; and ◦ managing our risk profile in order to protect our business.



[Your personal data](#)

[How we'll use your personal data](#)

[Who we share your personal data with](#)

[Other important information](#)

[Your rights](#)



Marketing & Advertising

Reason for data collection	Legal basis for collecting data
<p>To send you information and relevant advertising about our products and services and those of our trusted partners, including:</p> <ul style="list-style-type: none"> • sending you information about services which we think may interest you; and • to measure and analyse the impact of our advertising and marketing campaigns. 	<ul style="list-style-type: none"> • Consent to send you direct marketing by electronic message (e.g. email, SMS). • Legitimate interests in: <ul style="list-style-type: none"> ◦ effectively promoting our products and services, including measuring the effectiveness of our marketing campaigns and ensuring our marketing is relevant to you.
<p>You can change your marketing preferences at any point in the relevant preferences centre:</p> <ul style="list-style-type: none"> • if you're on the waitlist - use the 'Manage Consent' link in the 'Viral Loops' widget (depending on your cookie settings you may need to sign up again with the same email address to see this); • within the Zing app preferences once you have this set up; or • email us at support@zing.me (please note that it may take us up to 72 hours to act on your request if you submit your request by email). 	
<p>We'll still need to send you certain information, such as if there is a change to your terms and conditions, or if we need to tell you something to comply with our regulatory obligations.</p>	



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

Reason for data collection

Legal basis for collecting data

To personalise our products and services, including:

- tailoring our marketing messages and your Zing app to make them more relevant to you.

To do this, we may collect and analyse information about how you interact with our products and services, including the Zing app and your account, and about the transactions you make.

- Legitimate interest in understanding our customers, so that we can provide our customers, with a great user experience, and effectively promote our products and services;
- Consent (if given).

To improve our products and services, including the Zing app and our website, and to develop new products and services.

- Legitimate interest - in understanding our customers, so that we can improve existing, and develop new products and services in order to continue providing our customers with a great user experience and to grow our business;
- Consent.

To carry out market research, we, or another organisation acting on our behalf, may contact you to ask you for feedback/ to get involved in research.

- If you don't want to be contacted for market research then you can let us know privacy@zing.me.

- Consent - where required by law;
- Legitimate Interests - in understanding our customers and the market so that we can improve existing and develop new products and services in order to continue providing our customers with a great user experience and to grow our business.



[Your personal data](#)

[How we'll use your personal data](#)

[Who we share your personal data with](#)

[Other important information](#)

[Your rights](#)



Business/Administrative Purposes

Reason for data collection	Legal basis for collecting data
<p>To carry out back-office activities – including system development, audit, insurance, and administrative purposes.</p>	<ul style="list-style-type: none"> • Legal obligation; • Legitimate Interest - in ensuring the efficient administration of our business in accordance with applicable law and regulation.
<p>To protect our legal rights and comply with our legal and regulatory compliance obligations - this may include:</p> <ul style="list-style-type: none"> • sharing it with relevant authorities (for example, law enforcement or tax authorities); • in connection with legal proceedings; • to prevent or detect crime; • to support vulnerable customers; or • as otherwise necessary to allow us to protect any legal rights or comply with any other legal obligations. 	<ul style="list-style-type: none"> • Legal obligation; • Legitimate Interest - in complying with our legal and regulatory obligations in an effective and efficient manner. <p>To the extent this involves processing special categories of personal data:</p> <ul style="list-style-type: none"> • Substantial public interest • Explicit consent (we'll specifically ask for this if relying on this ground).

2.3 How we make decisions

We may use automated systems to help us make decisions, such as:

- fraud and money laundering checks; or
- assessing risks related to accounts.

These automated decisions aren't final. A human will usually investigate before any significant decision is made (such as denying your account application). In some circumstances, an automated decision might be made quickly (like freezing your account if suspicious activity is detected), but a human will always review it soon after.



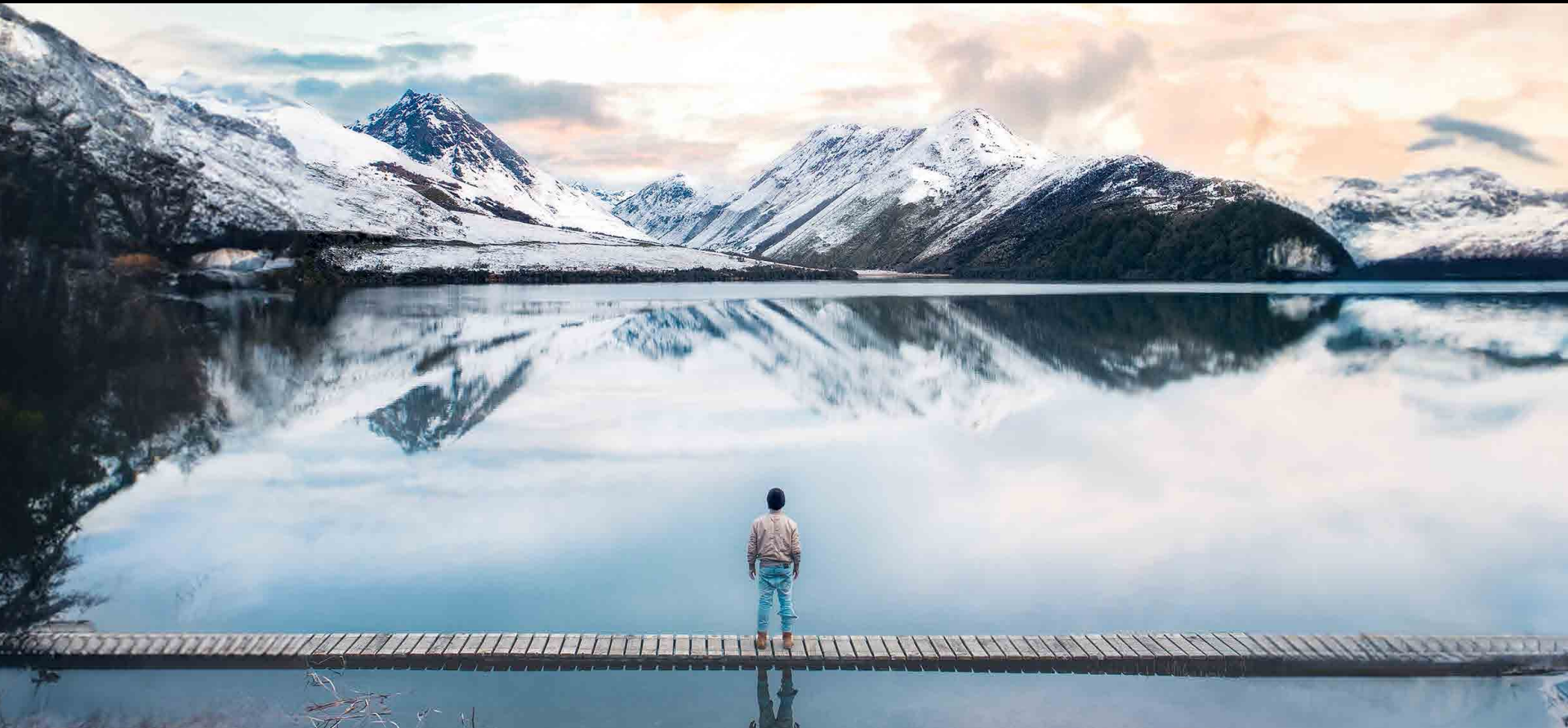
[Your personal data](#)

[How we'll use your personal data](#)

[Who we share your personal data with](#)

[Other important information](#)

[Your rights](#)



3. Who we share your personal data with

3.1 Who we share your personal data with

We may share your personal data with others if it's lawful. This includes where we or they:

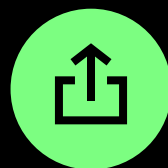
- need to so we can give you the products or services you've requested;
- need to for any regulatory reporting obligation, litigation, or to assert or defend legal rights or interests;
- have a legitimate business reason for doing so. This includes to confirm your identity, to manage risk or to check your suitability for products and services;
- have a public or legal duty to help with detecting and preventing fraud, tax evasion and financial crime; or
- have asked you for permission to share it, and you've agreed. It also includes where you've asked us to share it.



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

3.2 Third Parties we may share your personal data with

People/companies that you pay, or who make payments to you

Our Group Companies

This includes HSBC and HSBC Group Companies.

We will share data in connection with checks to prevent and detect crime and in our legitimate interests to run and protect our businesses and provide our services.

Service providers

- financial services providers, including international payment service providers and payment networks (including VISA and Mastercard);
- IT/cyber security providers such as those who provide payment services, analytics services, IT systems and hosting services, and our customer relationship and data management systems;
- organisations which help us to verify your identity, to carry out background checks and to prevent and detect crime. These include fraud reference agencies and screening service providers
- fraud prevention agencies who will also use it to detect and prevent fraud and other financial crime (see section [Fraud and Money Laundering](#) for more information on when we share data for fraud reasons);
- our professional service providers, such as auditors and legal advisors;
- service providers who help us:
 - provide payment services (including Checkout – our partner who lets you top up your account using your other cards, and CurrencyCloud)
 - provide ZingCare and other customer services
 - carry out surveys and promotions
 - communicate with you, including helping us send emails.



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

Online Advertising & Social media partners

We may share your personal data with our advertising and social media partners so that you're shown appropriate online adverts (see section ~~[X]~~ 3.2 for more information);

- Anyone you've agreed to us sharing, or have asked us to share, your personal data with
- This includes other Zing **members**. When you use the "Contact Sync" feature, you can see which of your contacts are also our Customers. You can learn more about this feature in the "How we'll use your personal data" section.
- Relevant public authorities

This includes law enforcement, the courts, dispute resolution bodies, and relevant regulators (both in the UK and overseas).

- Any parties involved in disputes, including disputed transactions
- Any relevant parties in connection with a partial or full, potential or actual merger, acquisition or takeover.

We may share aggregated or anonymised information within and outside of Zing with partners such as research groups, universities or advertisers. You won't be able to be identified from this information, for example, we may share information about general spending trends in the UK to help in research.

3.2 Social Media Audiences

We may share your contact details with social media companies in a 'hashed' format. Hashing is a security measure where the information is turned into a code. Social media companies can check if you have an account with them. If you do, you can ask them to:

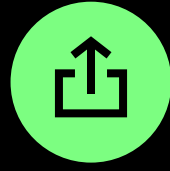
- use your information to send our adverts to you. For example, because:
 - we think that you might be interested in a new service that we offer to exclude you from receiving our adverts; or
 - the advert is for a service that you already use;



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



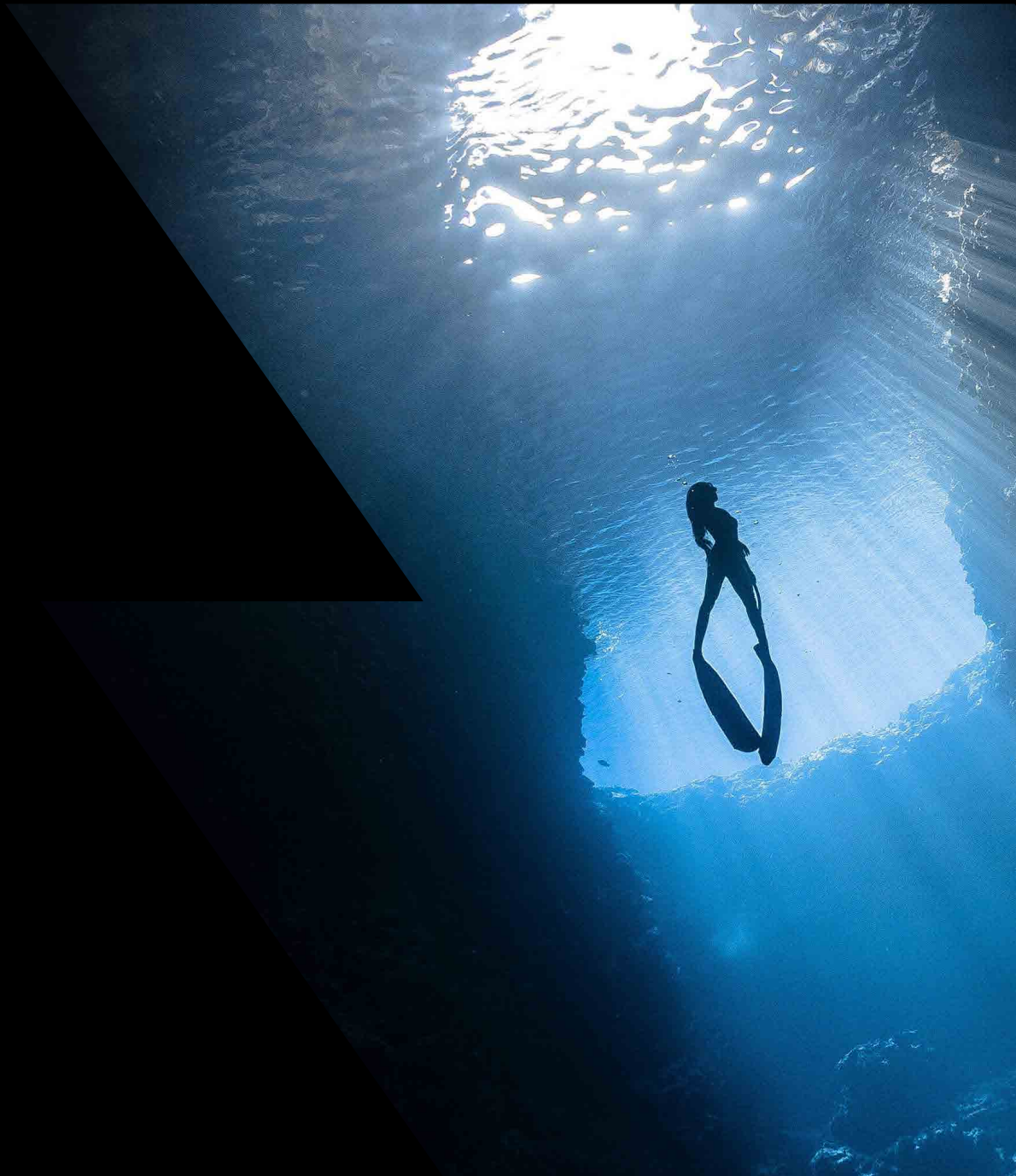
[Your rights](#)

- advertise to people who have a similar profile to you. For example, if we discover that one of our services is particularly useful to people with similar interests to the ones on your social media profile, we may ask our advertising partner or the social media network to send our adverts for that service to people who share your interests.

You can contact us if you'd like to opt-out of this data sharing. See "Your rights" [🔗](#).

You can also contact the social media platforms to:

- learn more about how they use your data for advertising;
- what controls they have in place to protect your data; and
- exercise your rights and preferences.





[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

If you've allowed us to use cookies that support our marketing, we and social media platforms can collect this information when you use our website. To learn more, or to switch this off, visit our Cookies Notice at [hsbc.co.uk/cookie-notice/](https://www.hsbc.co.uk/cookie-notice/). You can control which cookies you allow by selecting "Manage Cookies".

Facebook and TikTok

Meta Platforms Ireland is a 'joint controller' with us in law for processing where we collect information about you:

- from your actions on our Facebook page; or
- through the Facebook pixel on our website.

TikTok Information Technologies UK Limited, and TikTok Technology Limited (TikTok) are joint controllers with us in law where we collect information about you;

- from your actions on our TikTok account; or
- through the TikTok pixel on our website.

Where we are a joint controller we agree with the other party to share some responsibilities to protect your personal data, by:

- making sure we each have a legal basis for joint processing;
- honouring your legal rights in respect of your data; or
- ensuring security of joint processing.

You can ask us how we do this.

You can also contact Meta Platforms Ireland or TikTok about what they do. This includes exercising your legal rights in respect of the data they collect and keep data. Further details of how Meta Platforms Ireland processes your personal information, the legal basis it relies on, your rights and their contact details can be found at: [facebook.com/about/privacy](https://www.facebook.com/about/privacy).

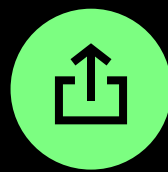
Further details of how TikTok processes your personal information, the legal basis it relies on, your rights and their contact details can be found at: [tiktok.com/legal/page/eea/privacy-policy/en](https://www.tiktok.com/legal/page/eea/privacy-policy/en).



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

Social Media Accounts

When you visit our page or account on social media sites we may collect data about you. This includes:

- **what you click on:** if you start a conversation;
- **what you view:** when you hover over a link or have an event page on screen;
- **what you say:** like comments or reactions;
- **your actions:** like sharing or recommending;
- **your location:** country or region. This is not your precise location unless you have provided this in your user profile and you're logged in your device and internet connection; and
- **your profile details and user ID.**

We have access to this information to use for reporting, insights and marketing purposes. This helps us improve our offering on social media and create better marketing. We may also see this information if we've communicated with you through social media. We do this because it helps us know who we're speaking to.

The social media site may also have access to this data, for example Meta Platforms Ireland can see this data when you visit our Facebook page.

3.3 Third party advertisers

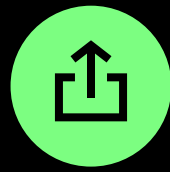
We and our advertising partners (such as social media providers) may use cookies. We do this to understand what you're interested in on our website, app and on social media. These ad companies may use what they learn about you to create a profile of your interests. They might then show you ads on other sites based on that. If you want more details about this, check out our Cookie Notice.



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

If you don't want these companies tracking what ads you see, you can turn it off:

- **For everyone:** You can stop these third-party cookies in your browser settings.
- **For iPhone users:** Go to Settings → Privacy & Security → Tracking and turn it off.
- **For Android users:** Go to Settings → Google → Ads → Opt out of ads personalisation and turn it off.

Remember, these settings can change depending on updates to your phone, so make sure to check your device's instructions if things look different.

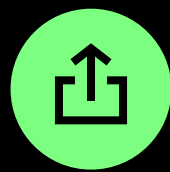




[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

3.4 Fraud and Money Laundering

Before we can give you access to our products and services, we have to carry out checks to make sure everything's legitimate. We work with fraud prevention agencies that help us spot any signs of fraud and money laundering. We'll also confirm your identity. To do these checks, we'll need to process personal data about you. This personal data might have been:

- provided by you;
- collected from you; or
- received from third parties.

We're mainly looking at things like:

- your name;
- where you live;
- your date of birth;
- how to contact you;
- your financial information;
- where you work; and
- information from your devices (like your identifiers such as IP address which is like an online address for your computer or phone).

Sometimes, we and the fraud prevention agencies we work with may let law enforcement agencies use your personal data. They'd use it to detect, investigate and prevent crime.

We process your personal data on the basis that:

- we have a legitimate interest in preventing fraud and money laundering; and
- to confirm your identity.

This allows us to protect our business and to comply with laws that apply to us.



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

Fraud prevention agencies can hold your personal data for different periods of time. If they think there's a risk you might be involved in fraud or money laundering, they could hold onto your data for up to 6 years.

Consequences of Processing

If we, or a fraud prevention agency, have reason to believe there's a fraud or money laundering risk, we may:

- refuse to provide the product or services you have requested; or
- stop providing existing products and services to you.

The fraud prevention agencies will keep a record of any fraud or money laundering risk. This record may be used to enhance fraud detection models. But it may also result in others refusing to provide services to you.

To find out more about our fraud prevention agencies and how they manage your information, please visit each agency directly:

- CIFAS - <https://www.cifas.org.uk/fpn>
- Action Fraud - <https://www.actionfraud.police.uk/privacy-information>
- National Crime Agency - <https://www.nationalcrimeagency.gov.uk/>
- RDC - <https://www.bvdinfo.com/en-gb/rdc-product-privacy-notice>
- LexisNexis (ThreatMetrix) - [add link when confirmed]



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data](#)



[Other important information](#)



[Your rights](#)



4. Other important information

4.1 How long we'll keep your information

We'll only keep your information in an identifiable form for as long as we need it. We'll only use it for the particular purpose we collected it. After that, we'll either delete it or change it so no one can tell it's about you.

For example, we'll normally keep your Financial and Relationship Data for:

- the duration of our relationship with you; and
- 5 years from when our relationship with you ends.

This allows us to:

- comply with our legal and regulatory obligations;
- use it for our legitimate purposes; and
- protect our legal rights. This includes dealing with any disputes or concerns that may arise.



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data](#)



[Other important information](#)



[Your rights](#)

4.2 Transferring your personal data overseas

Sometimes, your information may be sent to or stored (including being accessed from) locations outside the United Kingdom. When this happens, we ensure:

- appropriate safeguards are in place; and
- the transfer is in line with applicable legal requirements.

Certain countries have been approved by the UK Government as providing adequate protection for people's rights and freedoms in respect of their personal data. This means no additional safeguards are required to export Personal Data to these jurisdictions. A list of approvals is available [here](#).

For countries that haven't received this approval, we'll transfer it subject to United Kingdom approved contractual terms. These terms mean the recipient must follow the same data protection obligations. Sometimes, we can make the transfer without these extra steps, but only if the applicable data protection law permits this.

Fraud prevention agencies may also allow the transfer of your personal data outside of the UK. This may be to a country where the UK Government has decided that your data will be protected to UK standards. If the transfer is to another type of country, then the fraud prevention agencies will put appropriate safeguards in place to make sure your data continues to be protected.

Please contact us if you want to know more about:

- how your personal data is protected when it's transferred outside of the United Kingdom; and
- the safeguards we have in place.



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)



5. Your Rights

We think carefully about how we use your information. We always aim to use it in a way that's fair to you. You might prefer us not to use it for some purposes. You can exercise your rights by contacting us.

You have a number of rights relating to your personal data, including:

- **Access:** The right to access personal data we hold about you and to receive information about what we do with it;
- **Rectification:** The right to ask us to correct your information if it's inaccurate or incomplete;
- **Withdrawal of Consent:** The right to withdraw any consent you've given to any processing. This won't affect any previous processing carried out in reliance on such consent;
- **Erasure:** In some circumstances, the right to ask us to delete your information. We may, however still keep your information in certain circumstances, such as where we're required by law.
- **Objection/Restriction:** In some circumstances, the right to object to, and ask that we limit our processing of your information. This includes the right to object to any processing relying upon legitimate interests. There may however be situations where we're allowed to continue processing or refuse your request.



[Your personal data](#)



[How we'll use your personal data](#)



[Who we share your personal data with](#)



[Other important information](#)



[Your rights](#)

- **Portability:** In some circumstances, the right to receive the personal data you've given us in an electronic format and/or ask that we send it to a third party.

You can change your marketing preferences at any time.


Complaints

We aim to respond to all requests within 1 calendar month. If you're unhappy with how we handled your personal data, please get in touch.

You have a right to complain to the UK Information Commissioner's Office. You can do this by visiting ico.org.uk.

You may also have the right to complain to the data protection regulator in the country where you live or work.

Please contact us in the first instance so we can work with you to resolve your issue. You can contact our Data Protection Officer by emailing: DPO@zing.me.

This Privacy Notice may be updated from time to time, and the most recent version can be found at <https://wearemp.com/pdfs/PrivacyPolicy.pdf>. 

This notice was last updated in [DDth/st/Month/YYYY].