ZING

Privacy Notice

Information

Zing was closed on May 22, 2025

We closed the Zing app and service on 22nd May 2025 at 12:00 pm BST (midday) due to changes in strategic business priorities.

Zing's trading company, MP Payments UK Limited, and its group companies and service providers, (which is who we mean when we say "we" or "our") will retain your data to comply with our legal and regulatory obligations, in our legitimate interests to help manage our business during its wind-down period, and to protect our legal rights and interests.

Our privacy notice (in this document) continues to apply and provides more details about your rights and how we use your personal data. This does not change, except that:

- we will not use your personal data to provide or offer you financial products or services (except in certain limited situations connected with our wind-down, for example if you have disputed a transaction on your account or your card);

- we have stopped all marketing and advertising activities and your personal data will not be used for these purposes.

Our app has closed but you can continue to contact us at support@zing.me if you have any questions or want to contact us about your personal data.

Please download a copy of this notice for your records.

ZING

Privacy Notice (United Kingdom)

For peace of mind

We last updated this document on 2nd December 2024.



Contents



1. Your information



2. How we'll use your information



3. Who we share your information with



4. Other important information



5. Your rights

Welcome
1. Your information
2. How we'll use your information
3. Who we share your information with
4. Other important information
5. 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 like ours do this. We've put this notice together to explain what we do in more detail. Got questions? Reach out to us using the 'Get help' section of our app or by emailing us at support@zing.me.

When we talk about "we", "our" or "us" in this Privacy Notice we mean MP Payments UK Limited and our group companies involved in the provision of our services.



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 from third parties, such as fraud prevention agencies, group companies and our screening service providers.

We may also collect information about you using technology (such as cookies or pixels).

You can read more about how we collect your information here.

What we collect if you're a customer (or apply to be)

If you have (or have applied for) a Zing account 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 information we collect about you may be sensitive data.

What we may collect if you're a website visitor, waitlist member, or app user:

Marketing data (such as your preferences, feedback and opinions)

Technical data (information about your phone or browser)

Phone data (information on your phone that you've given us access to)

Analytics data (such as how you interact with the Zing app, website, or emails)

Find out more about what we collect here.

What we may collect if you're not a customer

For example if you're a connected or related party of a customer, a contact of a customer, someone who sends to or receives a payment from a customer, or someone who corresponds with us.

We may process information about you when your friend or family member opens an account with us, when a person you know shares their contacts with us, when you make a payment to a Zing account or when you receive a payment from a Zing account, or when you correspond with us.

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 information 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.

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 information overseas

Sometimes, your information may be sent to (including being accessed from or stored in) 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.

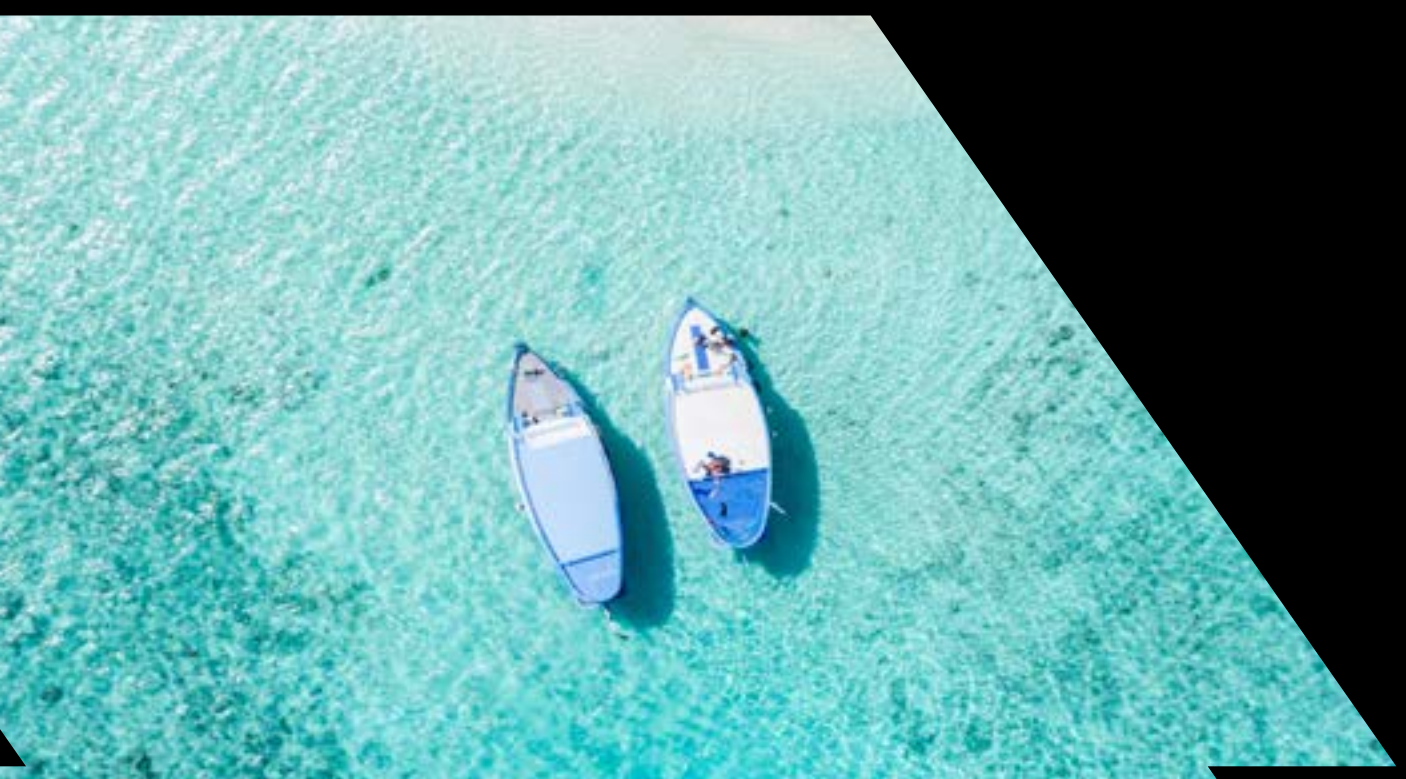
You find out more details about what happens to your information here.

Our commitment to you

We're committed to protecting your information. We use a range of technical, physical and organisational measures to help keep your information 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.

You can find more details about automated decisions here.

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 have a legal right to:

- ask us to provide you with copies of your information, make corrections or in some circumstances ask us to delete it
- tell us you no longer consent to us processing your information if you consented before
- object to our processing of your information (in some circumstances) or ask us to limit it or
- to ask for manual review of an automated decision (under certain circumstances).

You can find out more about your rights here.

We're not responsible for other services

We have links to other services on our own website or app. We don't own or operate these other services. 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.

Who's responsible for your information?

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

Complaints

If you're unhappy with how we've handled your 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 United Kingdom Information Commissioner's Office. You can do this by visiting https://ico.org.uk/global/contact-us.

This Privacy Notice may be updated from time to time. The most recent version can be found at zing.me/legal/privacy-notice.



Take your money global





1. Your information

1.1 How do we collect your information?

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, when you open an account or when you sign up to receive marketing. You must ensure that all information you share with us is correct and up to date. Please tell us as soon as possible of any changes.

We may also collect information about you when:

- you interact with us. For example, when you message us, change your details in the app, visit our website, fill in our surveys, use your card, enter our competitions or promotions, share information on social media with us, or use our app. We will ask you to agree to this collection, where appropriate.
- we have a duty to collect information to prevent financial crime and to comply with sanctions laws. We collect this from:
  - third parties such as fraud prevention agencies (see section "3.5. Fraud and Money Laundering")
  - other HSBC companies and
  - our screening services providers.

Information may be sourced from publicly accessible sources, such as Electoral Registers (either directly or indirectly). This information includes political affiliations, sanctions, and unlawful or criminal activities such as terrorism. Our third party providers may also use publicly accessible sources to check your address.

Cookies

Some of the information we collect 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 Cookies Notice.

Some of these uses are optional and so you'll be asked to agree to them first.

Emails

We also use technologies that are similar to cookies in our emails.
This lets us 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.

1.2 What information do we collect about you?

If you've applied for and when you use your 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).

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 information 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.

What we may collect if you're a website visitor, waitlist member, or app user:

- Marketing Data – information about the products and services you receive and your preferences, and where you have participated in market research activities, details of your feedback and opinions
- Technical data – information about your phone or browser, including the IP address, technical specifications such as operating system and browser version, and uniquely identifying information such as IMEI number
- Phone Data – information on your phone which you have given us permission to access, such as photos, geolocation data, and your address book
- Analytics data – information about how you interact with the Zing app, our website or our emails. Please see our Cookies Policy for further information.

When you receive or send a payment

We may process information about you, such as you name, when a person using Zing sends you a payment. We may also process information about you, such as your name, when you send a payment to someone with a Zing account.

When your correspond with us

We may process your contact details and information about your query and correspondence.

Connected persons

When a family member of a person you have a business relationship with applies for or holds an account with us, we carry out checks for fraud and crime prevention purposes. We may process information about you when we carry out these checks, which 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.



2. How we'll use your information

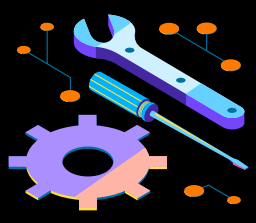
2.1 Lawful basis

We'll only use your information if:

Reason	Explanation	Lawful basis
The law makes us	We're legally required to collect this information, e.g., carrying out and keeping records of our anti-money laundering checks.	Legal obligation
We have a contract	To enter into or carry out an agreement we have with you.	Contractual necessity
You agree	You've told us we can use your information 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 or others have a legitimate interest	We or others 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

2.2 How we can use your information

We may use your information for the following reasons. We'll use one of the lawful basis identified:



Providing our products and services

Reason for data processing	Lawful basis
To verify your identity and to carry out background checks to: • prevent or detect crime, including fraud and financial crime and • comply with sanctions laws, including checking applications against certain fraud prevention and sanctions databases. 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. We may also use the photo you share with us during other customer's onboarding to check they're not fraudulent or duplicating your account.	• Legal obligation • Contractual necessity • Legitimate interest in: o preventing fraud and money laundering o confirming your identity in order to protect our business and o 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. If such information is 'special category' personal data, also: • Substantial public interest.
To check product eligibility: 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.	• Legitimate interest in: o managing our risk profile to protect our business and o complying with our legal and regulatory obligations in an effective and efficient manner.

Reason for data processing	Lawful basis
To provide and manage our financial products and services in line with our contracts and applicable laws and regulations: Financial services include: • moving money between wallets and • making payments.	• Legal obligation • Contractual necessity • Legitimate interest in: o providing our customers with great products and services and o complying with our legal and regulatory obligations in an effective and efficient manner.
To provide and manage the Zing app and our website, including: • 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. Where consent is collected to use a cookie or similar technology, you can withdraw this by changing your cookie settings. See our Cookies Notice for more detail on cookies.	• Legal obligation • Contractual necessity • Legitimate interest in: o providing our customers with great products and services o keeping our customers and their information safe o preventing fraud and money laundering and confirming your identity in order to protect our business and o complying with our legal and regulatory obligations in an effective and efficient manner. • Consent (if given).

Reason for data processing	Lawful basis
To provide you with optional functionality, such as matching your phone contacts to other Zing customers: Matching your phone contacts to other Zing customers 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. 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.	• Consent (if given).
To manage our relationship with you, including: • providing you with product and service updates and • customer support. 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. 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.	• Contractual necessity • Legitimate interest in: o providing our customers with great products and services o keeping our customers and their information safe o preventing fraud and money laundering, confirming your identity to protect our business and our customers, complying with applicable law and o complying with our legal and regulatory obligations in an effective and efficient manner. If such information is 'special category' personal data (for example, if you tell us about a health condition that affects your ability to use our services): • Substantial public interest.

Reason for data processing	Lawful basis
To prevent and detect crime, including fraud, money laundering, and terrorist financing through: • 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.	• Legal obligation • Legitimate interest in: o preventing fraud and money laundering in order to protect our business and our customers o complying with applicable laws and o managing our risk profile in order to protect our business. If such information is 'special category' personal data or information about criminal convictions or offences): • Substantial public interest.



Marketing & advertising

Reason for data processing	Lawful basis
To send you information and relevant advertising about our products and services and those of our trusted partners, including: • sending you information about services which we think may interest you and • to measure and analyse the impact of our advertising and marketing campaigns. You can change your marketing preferences at any point in the relevant preferences centre: • if you're on the waitlist - use the 'Manage Consent' link in the widget on the waitlist page (depending on your cookie settings you may need to enter your email address in the waitlist page again) • 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). Even if you don't agree to receive marketing, 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. For example, we might tell you about a new feature if we have a duty to make sure you're aware of it.	• Consent to send you direct marketing by electronic message (e.g. email, SMS) • Legitimate interest in: o effectively promoting our products and services, including measuring the effectiveness of our marketing campaigns and ensuring our marketing is relevant to you.

Reason for data processing	Lawful basis
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. Where consent is collected to use a cookie or similar technology, you can withdraw this by changing your cookie settings. See our Cookies Notice for more detail on cookies.	• 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 (if given).
To carry out market research, we, or another organisation acting on our behalf, may contact you to ask you for feedback or to get involved in research. • If you don't want to be contacted for market research then you can let us know at support@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.



Business/administrative purposes

Reason for data processing	Lawful basis
To carry out back-office activities – including system development, audit, insurance, and administrative purposes.	• Legal obligation • Legitimate interest – in ensuring the efficient administration of our business in accordance with applicable law and regulation.
To protect our legal rights and comply with our legal and regulatory compliance obligations – this may include: • 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.	• Legal obligation • Legitimate interest - in complying with our legal and regulatory obligations in an effective and efficient manner. To the extent this involves processing special categories of personal data: • 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 including building profiles about you.

A human will usually investigate before any significant decision is made (such as closing your account). In some circumstances, an automated decision might be made quickly (like freezing your account if suspicious activity is detected or stopping a suspicious card payment), and a human will then review it soon after. Where a significant decision is made without human review (for example, rejecting your account application), you have a right to certain information about how we make these decisions and to ask for the



decision to be made by a person instead of a computer. If this applies to you, we'll let you know, and explain how you can exercise this right.

3.1 Who we share your information with

We may share your information with others. This includes where we or they:

- need to do 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.

3.2 Third parties we may share your information with

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

We'll share data about you and your payment with people or companies you pay. This is required by law. When someone makes a payment to you we'll share details about you to confirm the payment is correct.

Our Group companies

This includes HSBC and HSBC Group companies.

We will share information in connection with checks to prevent and detect crime and to protect our businesses and provide our services.

Service providers

These include:

- financial services providers, including international payment service providers and payment networks (including Visa)
- 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 3.5. "Fraud and Money Laundering" for more information on when we share information for fraud reasons)
- our professional service providers, such as auditors and legal advisors
- service providers who help us:
  - provide payment services
  - provide ZingCare and other customer services
  - carry out surveys and promotions
  - communicate with you, including helping us send emails.

Online advertising and social media partners

We may share your information with our advertising and social media partners so that you're shown appropriate online adverts (see section "3.3. Social media audiences" for more information).

Anyone you've agreed to us sharing, or have asked us to share, your information with

This includes other Zing members. When you share your contacts with our app, you can see which of your contacts are also our Customers. You can learn more about this feature in section "2. How we'll use your information". We may also share your information with banks and other financial services providers of people you are paying, or people who are paying you, where necessary to help make sure the payment is made.

Relevant public authorities

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

Any parties involved in disputes, including disputed transactions

If we're involved in a dispute, we may share information about you as part of that dispute.

Any relevant parties in connection with a partial or full, potential or actual merger, acquisition or takeover

If we sell or propose to sell all or part of our business we might share your information with the buyer and their advisors.

Research groups, universities or advertisers

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 United Kingdom to help in research.

3.3 Social media audiences

We may share your contact details with social media companies so they can then check if you have an account with them. We'll do this securely to help protect your privacy.

If you do have an account, we can ask them to send our adverts to you. For example, they might use your information to send you adverts about things we think you might be interested in or new services we offer. They may also exclude you from receiving certain adverts. For example, if it's for a service you already use.

They may also advertise to people who have a similar profile to you (based on your social media profile). For example, we may ask our advertising partner or the social media platform to send our adverts for a service you use to people who share your interests.

You can contact us if you'd like to opt-out of this information sharing. See section "5. Your rights".

You can also contact the social media platforms to:

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

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.

Facebook and TikTok

Meta Platforms Ireland is a "joint controller" with us for processing where we collect or share information about you:

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

TikTok Information Technologies United Kingdom Limited, and TikTok Technology Limited (TikTok) are "joint controllers" with us where we collect or share 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 information, by:

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

You can ask us for more information about 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 information they collect and keep.

Further details of how Meta Platforms Ireland processes your information, the lawful basis it relies on, your rights and their contact details can be found at: facebook.com/about/privacy.

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

Social media accounts

When you visit our page or account on social media platforms we may collect information 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 isn't your precise location unless you have provided this in your user profile and you're logged into 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 platform may also have access to this information, for example, Meta Platforms Ireland can see this information when you visit our Facebook page.



3.4 Other third party advertisers

We and advertising companies we work with (including the social media providers set out above) may use cookies. We do this to understand what you're interested in on our website, app and on social media. These advertising 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 Cookies Notice.

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

- **For everyone:** You can stop these cookies in your browser settings or by using the website cookie pop-ups or other controls.

And in addition:

- **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.

3.5 Fraud and Money Laundering

We will carry out checks with fraud prevention agencies for the purposes of preventing fraud and money laundering, and to confirm your identity before we provide products and services to you. These checks require us to process personal data about you.

The personal data you have provided, we have collected from you, or we have received from third parties will be used to carry out these checks in order to prevent fraud and money laundering, and to verify your identity.

The personal data that will be processed include, your name, address, date of birth, contact details, financial information, employment details, and device identifiers such as IP address, as well as technical data about your device and information about how you use it.

Sometimes our providors will build up profiles from patterns in personal data and use it to help us identify whether an activity has come from you, or people pretending to be you. This helps us reduce fraud and crime.

We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data 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.

Fraud prevention agencies can hold your personal data for different periods of time and if you're considered to pose a fraud or money laundering risk, your data can be held for up to 6 years.

As part of the processing of your personal data, decisions may be made by automated means. This means we may automatically decide that you pose a fraud or money laundering risk if our processing reveals your behaviour to be consistent with money laundering or known fraudulent conduct, or is inconsistent with your previous submissions, or you appear to have

deliberately hidden your true identity. You have rights in relation to automated decision making: if you want to know more please contact us.

Where we decide that you pose a fraud or money laundering risk, this may result in significant consequences, including for example, rejecting your account application (please see Consequences of processing below). Where we make a significant decision by automated means, we will inform you of this, and explain how you can exercise your right to require us to manually review and reconsider our decision.

Consequences of processing

If we, the partners we use to help detect fraud, or a fraud prevention agency, have reason to believe there is a fraud or money laundering risk, we may refuse to provide the product or services or financing you have requested, or to employ you. We may also stop providing existing products and services to you and we may share it with other trusted providers.

A record of any fraud or money laundering risk may be kept by the fraud prevention agencies and partners. This record may be used to enhance fraud detection models, and share it with other trusted providers, and may also result in others refusing to provide services, financing or employment to you.

To find out more about these fraud prevention agencies and partners and how they manage your information, including how to exercise your rights, 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) - https://risk.lexisnexis.com/corporate/processing-notices/threatmetrix
- Onfido - https://onfido.com/privacy/



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 information 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.

4.2 Transferring your information overseas

Sometimes, your information may be sent to (including being accessed from or stored in) 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 United Kingdom government as providing adequate protection for people's rights and freedoms in respect of their information. This means no additional safeguards are required to export your information to these jurisdictions. A list of approvals is available here.

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

Fraud prevention agencies may allow the transfer of your personal data outside of the United Kingdom. This may be to a country where the United Kingdom government has decided that your data will be protected to United Kingdom standards, but if the transfer is to another type of country, then the fraud prevention agencies will ensure your data continues to be protected by ensuring appropriate safeguards are in place.



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 information, including:

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

- **Review of Automated Decisions**: where a significant decision (such as rejecting your account application) has been made without human review, you have the right to receive certain information about how we make such decisions and to ask us to manually review and reconsider our decision.

The United Kingdom Information Commissioner's Office has provided more guidance on what different rights are available to you here: A guide to lawful basis | ICO.

If you're unhappy with how we handled your information, please get in touch.

Withdrawing consent

You can change your marketing preferences at any time in the app under "Marketing Preferences", or if you're on the waitlist - use the "Manage Consent" link in the widget (depending on your cookie settings you may need to sign up again with the same email address to see this).

Where consent is collected to use a cookie or similar technology, you can withdraw this by changing your cookie settings. See our Cookies Notice for more detail on cookies. Where you have given consent to matching your phone contacts to other Zing customers this can be withdrawn in the app settings.

You can also withdraw consent at any time by contacting us at support@zing.me. Please note it may take up to 72 hours to act on your request if you submit your request by email.

Talk to us

Please contact us if you want to know more about:

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

You can also contact us for more information about how we process your information and we will reply in line with your legal rights. You can contact us at support@zing.me, or by contacting our Data Protection Officer at dpo@zing.me.

Complaints

We aim to respond to all requests within 1 calendar month.

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.

You have a right to complain to the United Kingdom Information Commissioner's Office. You can do this by visiting https://ico.org.uk/global/contact-us.

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

This Privacy Notice may be updated from time to time, and the most recent version can be found at zing.me/legal/privacy-notice.