Global Privacy Policy

13 September 2024

Global Privacy Policy

INTRODUCTION

IFX Payments (**IFX**, **we**, **us**, **our**) respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data and how the law protects you.

This privacy policy is provided in a layered format so you can click through to the specific areas set out below. Please also use the Glossary to understand the meaning of some of the terms used in this privacy policy.

1. IMPORTANT INFORMATION AND WHO WE ARE

PURPOSE OF THIS PRIVACY POLICY

This privacy policy aims to give you information on how we collect and process your personal data. This privacy policy is applicable if:

1. you communicate with us,
2. you, or a business you are associated with, registers for, or uses, any of our services, including indirectly through a customer of ours,
3. you subscribe to our marketing materials, including our Market Report, or engage with our marketing campaigns or competitions,
4. you interact with or use our website, ibanq, or our API,
5. you submit a complaint or a data rights request to us,
6. you, or your employer, provide services to us,
7. we carry out continuous due diligence, monitoring and screening, or respond to an external investigation, regarding anti-money laundering, politically exposed persons, source of wealth, fraud, sanctions or other criminal activities,
8. you report an error in, or request technical support for, ibanq or our API, or if you request any customer care support, or if we otherwise investigate an incident,
9. we process guarantee and indemnity claims,
10. you provide data for other legal and regulatory purposes or we otherwise process personal data to comply with our legal and regulatory obligations, or
11. in the appropriate circumstances, we enforce our rights against you (including our right to be paid).

The following are examples of individuals who this privacy policy applies to:

1. Affiliates, directors, shareholders, trustees, employees, and any other individuals associated with our active or prospective clients, as identified in documents provided to us or sourced by us during our onboarding process.
2. Any individual whose personal data we process for providing or potentially providing our services, including through communications, interactions, and transactions, to comply with legal obligations like verification and anti-money laundering checks. This includes customers of our customers and individuals involved in transactions.
3. Any individual whose personal data we process related to the provision of services to us, including employees, contractors, and representatives of our suppliers and partners.

It is important that you read this privacy policy together with any applicable schedules and any other policies or notices we may provide on specific occasions when we are collecting or processing personal data about you. This privacy policy supplements the applicable schedules together with other policies and notices we may issue from time to time and is not intended to override them.

OUR ROLE

IFX is made up of different legal entities (our **Group**). IFX (UK) Ltd generally acts as the entity responsible for determining the purposes and means of processing personal data. However, for certain processing activities necessary to provide our services, we may instruct a member of our Group to process data, or share joint control over the data with our customers (which we call a **Third Party Entity**). In other instances, we may operate as a data processor, carrying out processing on behalf of a Third Party Entity in accordance with their specific instructions.

If you require additional details about the scenarios in which we act as a joint controller of your personal data, or the parties with whom we share such joint control, please reach out to us directly. Similarly, if you have questions about how a Third Party Entity processes your information, you should contact that specific Third Party Entity for more information.

CONTACT DETAILS

We have appointed a Data Protection Officer who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact us using the details set out below.

Email: privacy@ifxpayments.com
Postal address: IFX Payments, 33 Cavendish Square, London, W1G 0PW, United Kingdom

We are registered with the Information Commissioner's Office (**ICO**) (Reference Number: Z9399766). You have the right to make a complaint at any time to the ICO, the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance.

CHANGES TO THIS PRIVACY POLICY AND YOUR DUTY TO INFORM US OF CHANGES

We may update or modify this privacy policy periodically, including to account for any changes in our personal data processing practices or to reflect developments in applicable laws. Any revisions to this privacy policy will be published on our website. We encourage you to review this privacy policy regularly to stay informed of the latest changes.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

2. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (i.e. anonymous data).

We may collect, use, store and transfer different kinds of personal data, as outlined below. The following paragraphs are notice of the collection of the following categories of personal data under applicable law:

- **Identity Data** includes first name, last name, title, date of birth, employer, details on a business card or in an email signature, nationality, political exposure status or family relationship to a politically exposed person, passport and other forms of identification (such as utility bills, social security number, national insurance number, tax identification number, residence permit, payslips, firearms license/certificate, electoral register information, credit/debit card statement, council tax bill, or any other document from a governmental body or agency), residence country, gender, maiden name, marital status, job title, role, shareholding details, birth certificate, marriage certificate, national ID card, driving license, company/organisation name, socio-demographic information, Curriculum Vitae, sanction-related information, education background, directorship.

- **Contact Data** includes your residential or shipping address, previous addresses, email addresses, mobile numbers, telephone numbers and other information available in an email signature.

- **Financial Data** includes bank account information, including account holder, account name, account number, unique identifier, reference details, sort code, account balance information, and details regarding your financial status, assets, income, salary information, bank statements, and source of wealth information.

- **Transaction Data** includes details of payment transactions, including account number, account name, country of birth, account description, ultimate remitter and remitter, contact information (e.g., email address), unique identifier, country of residence, sort code, service user name, ultimate beneficiary and beneficiary, payment amount, ID (e.g., passport/driving license), ultimate debtor address, cheque amount and serial number, message identifiers, and any data contained in a payment reference, or included in a free text field, which may include sensitive personal information and details related to hobbies, interests or activities.

- **Technical Data** includes internet protocol (**IP**) address, language and country settings, browser type and version, time zone setting and location, hardware capabilities and screen information, browser plug-in types and versions, operating system, type of device, unique device identifier (e.g. MAC or IMEI number), network information and other device related information.

- **Security Data** includes your username and password, and any other authentication data you may use to access your accounts (such as a security passphrase, memorable work, first access PIN or "hints" associated with them).

- **Usage Data** includes anonymous analytical data about how you use our website and services. This includes information such as your IP address, the pages of our website that you visit and usage information obtained via the use of cookies.

- **Marketing** and **Communications Data** includes your preferences in receiving marketing from us, your communication preferences and any feedback or survey responses you may issue to us from time to time.

- **Phone Call Data** includes recordings of inbound or outbound phone calls between you

and us, including an transcriptions of the same.

- **Publicly Available Data** includes information gathered from online searches or other public records, including identity details, socio-demographic information, financial and economic data, data from the electoral register and Companies House, as well as negative media coverage.

- **Correspondence Data** includes details you provide in, or we gather about you from, any correspondence or communication with us, including information about any enquiries or requests for technical assistance and any complaints.

- **Biometric Data** includes your facial biometrics, which may include a "selfie" taken on your mobile or other device holding a copy of your identification documents, or a photo or video captured during an identity verification session.

We also collect, use and share aggregated data (**Aggregated Data**) such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

We may process and record information on criminal convictions, including terrorism and fraud. This data may be shared with financial crime prevention agencies, law enforcement, regulators, and other financial institutions.

We may inadvertently process some special categories of personal data (other than Biometric Data and criminal conviction data), such as race, ethnicity, religious beliefs, sexual orientation, political opinions, trade union membership, health, and genetic information. This data can be transferred to us unknowingly through payment references or free text fields, or we may obtain it during money laundering and verification checks.

We may process confidential and sensitive information about individuals identified by Third Party Entities as vulnerable or at risk, who need to be opted out of the Confirmation of Payee (CoP) Service.

IF YOU FAIL TO PROVIDE PERSONAL DATA

If we are legally required to collect personal data, or if it is necessary under the terms of a contract with you (or a Third Party Entity), and you do not provide the requested data, we may be unable to fulfill or enter into that contract (e.g. to provide services to you or the Third Party Entity). In this case, we may have to cancel a service you have with us but we will notify you if this is the case at the time.

3. HOW IS YOUR PERSONAL DATA COLLECTED?

We use different methods to collect data from and about you including through:

- **Direct interactions.** You may give us or our third-party providers your Identity, Contact, Financial, Phone Call and Biometric Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you (or a Third Party Entity):

  - apply for our services,
  - create an ibanq account or register as an ibanq user,
  - take part in any competition or promotion organised by us,
  - request marketing materials to be sent to you, or
  - give us feedback or contact us.

- **Automated technologies or interactions.** As you interact with ibanq and our website, we may automatically collect Technical Data and Usage Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data and Usage Data about you if you visit other websites employing our cookies. Please see our Cookie Policy for further details.

- **Third parties or publicly available sources.** We may receive personal data about you from various third parties and public sources as set out below:

  - Technical Data from the following parties (based in or outside of the UK):
    (a) analytics providers,
    (b) advertising networks,
    (c) search information providers, and
    (d) identity verification providers.

  - Identity, Contact, Financial and Transaction Data from:
    (a) UK and overseas government and regulatory bodies, including the Financial Conduct Authority, the Financial Ombudsmen Service, HM Revenue and Customers and the National Crime Agency,
    (b) Bailiffs and debt collection agencies,
    (c) Third Party Entities,
    (d) Payment service providers, financial institutions, intermediaries, payment system operators (including SEPA, Faster Payments, CHAPS, BACS), other financial services companies (to process payments, facilitate foreign exchange orders and prevent, detect, and prosecute fraudulent and criminal activities), and external advisors,
    (e) Credit reference agencies,
    (f) LexisNexis Risk Solutions (**LNRS**), who manage a global shared intelligence network known as the ThreatMetrix Digital Identity Network (**DIN**). The DIN collects and processes intelligence from millions of daily interactions including logins, payments and new account applications across thousands of DIN participants, with the aim of preventing and reducing fraud.

  - Publicly Available Data from public registers including third-party websites.

  - Identity and Contact Data from data brokers or aggregators based inside or outside the UK.

4. HOW WE USE YOUR PERSONAL DATA

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you or a Third Party Entity.

- In order to receive services from a third-party supplier with whom you are associated with.

- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

- Where we need to comply with a legal or regulatory obligation.

- Where we have your consent to do so (which may be obtained by a Third Party Entity on our behalf).

Generally we do not rely on consent as a legal basis for processing your personal data other than in relation to (a) sending marketing communications to you, (b) collecting consent to cookies or (c) where it is appropriate to do so in the circumstances. You have the right to withdraw consent to the processing of personal data at any time by contacting us at privacy@ifxpayments.com.

As mentioned above, we may inadvertently process some special categories of personal data, such as race, ethnicity, religious beliefs, sexual orientation, political opinions, trade union membership, health, and genetic information. This information can be transmitted to us through payment references or free text fields, or we may obtain it during money laundering and verification checks. We process these special categories of personal data on the basis that this data has been manifestly made public by the data subject.

We process Biometric Data and some other special categories of personal data (such as information on criminal convictions related to fraud and terrorism) on the basis that the substantial public interest exemption in preventing fraud and money laundering applies. We have appropriate policy documents in place the govern the processing of this data.

PURPOSES FOR WHICH WE WILL USE YOUR PERSONAL DATA

The table below sets out a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new customer, or an ibanq user.	(a) Identity (b) Contact (c) Correspondence (d) Financial (e) Usage (f) Security (g) Technical (h) Marketing and Communications (i) Publicly Available	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to operate our business, provide our services and fulfil our contractual and legal obligations)
To provide our services, including: (a) managing transactions such as payments and foreign exchange orders via telephone,	(a) Identity (b) Correspondence (c) Contact (d) Financial (e) Technical (f) Transaction (g) Marketing and	(a) Performance of a contract with you. (b) Necessary to comply with a legal obligation. (c) Necessary for our legitimate interests (to provide our services,

(b) providing access to ibanq and Mass Payments.	Communications (h) Phone Call (i) Correspondence (j) Usage (k) Security (l) Publicly Available	operate our business and fulfil our legal and contractual obligations).
To manage our relationship with you which will include: (a) notifying you about changes to our services or our terms and conditions, (b) responding to requests for technical support and dealing with complaints, and (c) asking you to leave a review or take a survey about our services.	(a) Identity (b) Contact (c) Usage (d) Transaction (e) Correspondence (f) Security (g) Technical (h) Marketing and Communications (i) Phone Call	(a) Performance of a contract with you. (b) Necessary to comply with a legal obligation. (c) Consent. (d) Necessary for our legitimate interests (to keep our records updated, to understand how customers use our products/services, to address customer queries and to keep customers informed of changes to our services).
To manage our business, including: (a) maintaining financial records, conducting audits, performing testing, and complying with corporate governance and reporting requirements, (b) enforcing contractual rights, including debt recovery, and (c) supporting internal reporting and management information needs.	(a) Identity (b) Contact (c) Usage (d) Transaction (e) Correspondence (f) Security (g) Technical (h) Phone Call	(a) Performance of a contract with you. (b) Necessary to comply with a legal obligation. (c) Necessary for our legitimate interests (to exercise our rights, including to recover debts owed to us, to provide our services and to fulfil our legal and contractual duties).
To market our services, including to: (a) deliver relevant website content and advertisements to you, (b) measure and understand the effectiveness of the advertising we present to you, and (c) run campaigns and competitions, including through partnerships with our affiliates.	(a) Identity (b) Contact (c) Marketing and Communications (d) Usage	(a) Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy). (b) Consent.
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences.	(a) Technical (b) Usage (c) Identity (d) Contact (e) Correspondence (f) Transaction (g) Technical (h) Marketing and Communications	(a) Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy). (b) Consent (specifically for cookies).
To perform the following compliance functions: (a) conduct due diligence, verification and anti-money laundering checks, (b) detect, investigate and report fraud and criminal activities including responding to legal and law enforcement requests, (c) ensure security, manage risks and prevent crime through continuous monitoring and screening of transactions, customers and payments, and (d) fulfil our legal obligations.	(a) Identity (b) Contact (c) Transaction (d) Financial (e) Phone Call (f) Correspondence (g) Security (h) Usage (i) Publicly Available (j) Biometric	(a) Necessary to comply with a legal obligation. (b) Necessary for our legitimate interests and those of our customers (to verify the identity of our customers, to detect and prevent fraud, money laundering and other criminal activity and fulfil our legal obligations). (c) Necessary in the public interest (for detection and prevention of fraud and money laundering). (d) Necessary the establishment, exercise or defence of legal claims.
To administer and protect our business and our website (including troubleshooting, incident management, data analysis, testing, system maintenance, support, reporting and hosting of data). To manage our supplier relationships, such as with our banking partners, advisors and other intermediaries.	(a) Identity (b) Contact (c) Technical (d) Phone Call (e) Financial (f) Correspondence (g) Usage (h) Security (i) Transaction	(a) Performance of a contract with you. (b) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, and improving our products and services). (c) Necessary to comply with a legal obligation.

MARKETING

Where we obtain your consent to send you marketing communications, you can unsubscribe by following the unsubscribe link within the communication. Where marketing consent is gained through the acceptance of cookies, opt-out can be managed via the cookie preferences banner.

If you have requested information or purchased services from us, and you have not opted out of receiving that marketing, where permitted by law, we may contact you by email or other electronic means. You can adjust your preferences and/or opt-out of marketing at any time. Just click on the unsubscribe links on any marketing message we send you or email us at privacy@ifxpayments.com.

THIRD-PARTY MARKETING

We will obtain your express opt-in consent before we share your personal data with any company outside our Group for marketing purposes.

COOKIES

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of our website or ibanq may become inaccessible or not function properly. For more information about the cookies we use, please see our Cookie Policy.

Please note that the DIN operates by the use of cookies (please refer to our Cookie Policy, with reference to the cookie "thx_guid"). Your personal data may be processed by LNRS as a controller (or otherwise) in accordance with their processing notices, available here: https://risk.lexisnexis.com/corporate/processing-notices

CHANGE OF PURPOSE

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to receive an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. DISCLOSURES OF YOUR PERSONAL DATA

We may have to share your personal data with the parties set out below for the purposes set out in the table in paragraph 4 above:

- "Internal third parties" as set out in the Glossary.
- "External third parties" as set out in the Glossary.
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy policy.

We require all third parties to respect the security of your personal data and to treat it in accordance with applicable law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

6. INTERNATIONAL TRANSFERS

Members of our Group and some of our external third parties are based outside the UK and the European Economic Area (**EEA**) so their processing of your personal data may involve a transfer of data outside the UK and the EEA. We will take all reasonable steps to make sure that your personal data is handled securely and in line with this privacy policy and applicable laws. In many circumstances, we will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data. When making international transfers of your personal data, we may also use specific contracts approved for use in the UK which give personal data the same protection it has in the UK.

It is important to understand that some countries are not automatically deemed to have adequate legal protections for personal data or individual data subject rights. In particular, we may transfer your data to our Group company in the Dubai International Financial Centre (**DIFC**). Our third-party banking partners in other jurisdictions (including the USA) may also need to process your personal data in connection with the services provided to you or any Third Party Entity.

In relation to transfers to these countries, we may transfer personal information through the use of International Data Transfer Agreements and Standard Contractual Clauses or other measures as required. All of your personal information will be afforded a high level of protection wherever it is processed and no matter whether it is held by us, our Group companies, our contractors or agents.

Please contact us if you want further information on the specific mechanisms used by us when transferring your personal data out of the UK.

7. DATA SECURITY

We have implemented technical and organisational measures to protect your personal data from being accidentally lost, used or accessed in an authorized way, altered or disclosed. These include:

- encryption in transit and at rest to ensure an appropriate level of security,
- measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that we operate,
- measures that allow us to backup and archive appropriately in order to restore availability and access to our your data in a timely manner in the event of a physical or technical incident, and
- processes for regularly testing, assessing and evaluating the effectiveness of certain key technical and organisational measures we implement.

In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breaches and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. DATA RETENTION

HOW LONG WILL YOU USE MY PERSONAL DATA FOR?

To comply with our obligations under applicable anti-money laundering regulations, we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for at least five years from (a) the date of a completed transaction or (b) when our business relationship has come to an end. We are not required to retain transaction records over the course of our business relationship for more than ten years.

In some circumstances you can ask us to delete your data: see "request erasure" below for further information.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

9. YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under applicable data protection laws in relation to your personal data. You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy, (b) where our use of the data is unlawful but you do not want us to erase it, (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims, or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine- readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent. There may also be circumstances where your consent cannot be withdrawn for legal or regulatory reasons.

If you wish to exercise any of the rights set out above, please contact us.

NO FEE USUALLY REQUIRED

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

WHAT WE MAY NEED FROM YOU

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

TIME LIMIT TO RESPOND

We try to respond to all legitimate requests within **one month**. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. GLOSSARY

LAWFUL BASIS

Legitimate interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of a contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal or regulatory obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

THIRD PARTIES

Internal third parties means other companies within our Group acting as joint controllers or processors, such as our Group companies in Poland or the DIFC.

External third parties means:

- Service providers acting as processors who provide compliance, IT, identity

authentication, and system administration services.

- Third Party Entities.
- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers who provide consultancy, legal, insurance and accounting services.
- Our third party banking, liquidity and financial services partners.
- UK and overseas government and regulatory bodies, including the Financial Conduct Authority, the Financial Ombudsmen Service, HM Revenue and Customers and the National Crime Agency, who act as processors or joint controllers who require reporting of processing activities under certain circumstances.

A complete list of the third parties who we engage to process personal data on our behalf, together with the location of processing, is available on our website at https://www.ifxpayments.com/data-privacy/.

SCHEDULE 1 – APPLICABLE TERMS FOR RESIDENTS IN CANADA

This information applies if you are a resident in Canada. Please read this schedule carefully, as the information in it takes precedence over the information provided to you in our privacy policy.

The following information in our privacy policy is amended and supplemented as follows:

OUR ROLE

For Canadian residents, your personal information is under the custody and control of IFX (UK) Ltd.

HOW WE USE YOUR PERSONAL DATA

IFX (UK) Ltd collects, uses and discloses your personal data for the purposes identified in our privacy policy and with your express or implied consent, except as otherwise permitted or required by applicable law. When we collect and process your sensitive data, we will obtain your express consent in writing or by electronic means and use it only for the purpose necessary to conduct our business in an appropriate manner or as permitted by applicable law and guidelines.