Privacy Policy
KP PAY LIMITED

Effective as of 01/04/2023

kp pay

Privacy Policy . **KP PAY LIMITED**

Who we are

We are KP PAY LIMITED of 483 Green Lanes, London, N13 4BS ("KP PAY", "we", "us", "our"), authorised by the Financial Conduct Authority (FCA) to carry on electronic money activities under the Electronic Money Regulations 2011 (EMRs).

We're registered with the Information Commissioner's Office (ICO) under number ZB231756.

Our contact details

Phone Number: +447311897973
E-mail: info@kppay.co.uk

The type of personal information we collect

We may collect and process all or any of the following information:

- your name, address, and date of birth
- your email address and phone number
- copies of your identification documents (for example, your passport or driving license) and any other information you provide to prove you are eligible to use our services
- your country of residence, tax residency information and tax identification number
- details of the relevant business account you are associated with, including the account number, sort code and IBAN
- records of our discussions, if you contact us or we contact you (including records of phone calls)
- your image in photo or video form (where required as part of our Know-Your-Customer (KYC) checks, or where you upload a photo to your account)
- information about other people (such as the company's shareholders, directors, employees, customers or business partners) where we are legally required to ask for such information (for example, as part of KYC checks or under anti-money laundering laws to verify your company's sources of funds)

Where you, or your company, give us personal data about other people, you are responsible for ensuring that they understand how we will process their personal data.

Separately from other data, there are specified category of data as cookies. We are using cookies when you are using our web based platforms (e.g. browsing websites, applications of KP Pay, sending email and text messages, communicating through social media accounts). The cookies mostly relate to the necessity of providing services you have explicitly requested (e.g., to open a website or some section of it, making payments etc.) or your authentication during the login process.

Additionally, when you are visiting our websites, we may collect certain information automatically from your device in order to provide services requested by you, ensure security and for statistical purposes.

How we get the personal information and why we have it

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- to verify your identity and eligibility, when you apply to use our products, and decide whether or not to approve your application;
- to use our products or services (for example, to make payments into and out of your account);
- to use our customer support services;

We also receive personal information indirectly, from the following sources in the following scenarios:

- Information collected from your use of our website and application:

  - technical information, including the internet protocol (IP) address used to connect your computer to the internet, your log-in information, the browser type and version, the time-zone setting, the operating system and platform, the type of device you use, a unique device identifier (for example, your device's IMEI number, the MAC address of the device's wireless network interface, or the mobile phone number used by the device), mobile network information, your mobile operating system and the type of mobile browser you use
  - information about your visit, including the links you have clicked on, through and from our website or app (including date and time), services you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling and clicks), and methods used to browse away from the page
  - information on transactions (for example, payments into and out of your account), including the date, time, amount, currencies, exchange rate, beneficiary details, IP address of sender and receiver, sender's and receiver's name and registration information, messages sent or received, details of device used to arrange the payment and the payment method used.

- We may collect personal data from third parties, such as credit reference agencies, financial or credit institutions, official registers and databases, as well as fraud prevention agencies and partners who help us to provide our services
- We may collect information about you if you make it publicly available on websites, social media websites or apps. We only do this as part of our KYC checks.
- We may collect, or may ask you to provide, personal data from publicly available sources, such as media stories, online registers or directories, and websites for enhanced due diligence checks, security searches and KYC purposes.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing this information are:

- **Keeping to our contracts and agreements with you**

We need certain personal data to provide our services and cannot provide them without this personal data.

- **Legal obligations**

In some cases, we have a legal responsibility to collect and store your personal data (for example, under anti-money laundering laws we must hold certain information about our customers).

- **Legitimate interests**

We sometimes collect and use your personal data because we have a legitimate interest to use it and this is reasonable when balanced against your right to privacy.

- **Substantial public interest**

Where we process your personal data, or your sensitive personal data (sometimes known as special category personal data), to adhere to government regulations or guidance.

- **Consent**

Where you've agreed to us collecting your personal data, or your sensitive personal data, for example when you have ticked a box to indicate that you are happy for us to use your personal data in a certain way.

We use the information that you have given us in order to:

- verify your identity and eligibility, when you apply to use our products, and decide whether or not to approve your application;
- meet our contractual and legal obligations relating to any products or services you use (for example, making payments into and out of your account);
- provide you with customer support services;
- check your identity and to protect against fraud, keep to financial crime laws and to confirm that you are eligible to use our services;
- offer you and new products and services that might interest you;
- manage our website and application (including troubleshooting, data analysis, testing, research, statistical and survey purposes);
- prepare anonymous statistical datasets about our customers' spending patterns:
    - for forecasting purposes
    - to understand how customers use our services
    - to comply with governmental requirements and requests

These datasets may be shared internally or externally with others. We produce these reports using information about you and other customers. The information used and shared in this way is never personal data and you will never be identifiable from it. Anonymous statistical data cannot be linked back to you as an individual.

How and why we can share the personal information with third parties

We may share this information with share it with other organisations (for example, government authorities, law enforcement authorities, tax authorities, fraud prevention agencies), when we are bound to do so by law, in connection with legal claims, or to help detect or prevent crime.

We may also share your personal data with our affiliates, business partners, suppliers and subcontractors for the performance and execution of any contract we enter into with them or you and to help them improve the services they provide to us, and with our group entities and subsidiaries.

When we transfer your personal data to the third parties, we operate as controllers[1] of personal data, and the parties we transfer the personal data to, operate as processors[2].

In order to keep our services more affordable and our business more efficient, we may transfer your data to and store it in countries outside of the UK and the EU. It may also be processed by staff operating outside of your jurisdiction. Such staff may be engaged in activities that include the fulfilment of your payment order, the processing of your payment details and the provision of support services. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Policy.

When we transfer your personal data to third parties as processors, we ensure that appropriate safeguards, including Standard Contractual Clauses and/or International Data Transfer Agreements, are in place. As the controllers, we are also responsible for the compliance of our processor(s).

By using our services, you confirm that you understand and consent to the disclosure to the third parties and processing of your personal data (or the personal data of any individual you provide) as described in this Privacy Policy.

[1] a controller is a person that exercises overall control of the purpose and means of the processing of personal data and is responsible for the compliance with all the data protection principles as well as the other UK GDPR requirements.

[2] A processor is a person processing the personal data for different purposes, but always on behalf of, and on the instructions of, the relevant controller.

How we store and protect your personal information

Your information is securely stored. Only a small number of our employees can see your personal data, and they'll only look at it if they absolutely need to. We always delete information that we no longer need. And everything we need to keep is subject to the highest levels of security.

We use a variety of physical and technical measures to:

- keep your personal data safe
- prevent unauthorised access to your personal data
- make sure your personal data is not improperly used or disclosed

Electronic data and databases are stored on secure computer systems with control over access to information using both physical and electronic means. Our staff receives data protection and information security training. We have detailed security and data protection policies which staff are required to follow, when they handle your personal data.

We use HTTPS (HTTP Secure), where the communication protocol is encrypted through Transport Layer Security for secure communication over networks, for all our app, web and payment-processing services.

While we take all reasonable steps to ensure that your personal data will be kept secure from unauthorised access, we cannot guarantee it will be secure during transmission by you to our app, a website or other services.

If you use a password for our application or website, you will need to keep it confidential. Please do not share it with anyone.

When you use our public services, which includes our social network accounts, please do not share any personal data that you don't want to be seen, collected or used by other customers, as this personal data will become publicly available.

How long we store your personal information and how we dispose of it after we no longer need it

We will generally keep your personal data for six years after our business relationship ends or such period as may be required by applicable local laws.

We are required to keep your personal data for this long by anti-money laundering and e-money laws. We may keep your personal data for longer because of a potential or ongoing court claim or another legal reason.

We will then dispose of your information by electronic and physical methods, such as shredding, destruction and secure disposal of hardware and hard-copy records, and deletion or over-writing of digital data.

We do this automatically upon expire of the mandatory data retention period, so you don't need to contact us to ask us to delete your data.

Your data protection rights

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at info@kppay.co.uk or by calling our hotline: +447311897973 if you wish to make a request.

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us by email at info@kppay.co.uk or by calling our hotline: +447311897973.

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk