

ExePay Limited Privacy Notice

Contents

1 Who “we” are.....	1
2 Information collected from others	2
3 What Personal Data do we collect?.....	2
4 How we obtain information	3
5 Credit reference and fraud prevention agencies	4
5.1 General.....	4
5.2 Automated Decisions	4
5.3 Consequences of Processing	4
5.4 Data Transfers	4
6 How Do We Use Your Personal Data?	5
7 Schedule of Purposes of Processing	5
7.1 Contractual necessity	5
7.2 Legal obligation.....	5
7.3 Legitimate interests	6
8 Marketing information	8
9 Transferring information overseas.....	8
10 What Special Categories of Personal Data Do We Process?	9
11 When Do We Share Client Personal Data?	9
12 How Long Will My Personal Data Be Retained?	10
13 How is my Personal Data secured?	11
14 Your rights.....	11
15 No fee usually required.....	13
16 What we may need from you.....	13
17 Where Can I get Further Information?	13

1 Who “we” are

ExePay Limited (“ExePay”, we”, “us”, “company” or “our”) is committed to protecting the privacy and security of your Personal Data.

This Privacy Notice applies to all personal information processing activities carried out by about you prior to, during and after your client relationship with us. It is relevant to anyone

who uses our services, including customers, prospective customers, suppliers, contractors, and website users.

Our principle address is 5 Stratford Place, London, England, W1C 1AX.

We may update our Privacy Notice from time to time. When we do, we will communicate any changes by publishing the updated Privacy Notice on our website. We would encourage you to visit our website regularly to stay informed of the purposes for which we process your information and your rights to control how we process it.

2 Information collected from others

Where we have collected information directly from you it will usually be obvious what this is, as you will have given it to us. This might not be the case where we have used cookies to collect information from your computer or portable devices. Please see our Cookies Policy for more information.

3 What Personal Data do we collect?

We respect individuals' rights to privacy and to the protection of personal information. The purpose of the Privacy Notice is to explain how we the data controller collect and use personal data in connection with our business. "Personal Data" means information about a living individual who can be identified from that information (either by itself or when combined with other information). We will collect and process various categories of personal data at the start of and for the duration of, your relationship with us. We will limit the collection and processing of information to information necessary to achieve one or more legitimate purposes as identified in this notice. Personal data may include:

- personal contact information (including your name, home address, personal telephone number(s) and personal e-mail address);
- business contact information (including e-mail address and telephone number);
- date of birth;
- social security, government identification and / or driving licence number;
- gender;
- copy of your passport, visa or driving licence;
- company account details, tax residence and tax status information;
- copies of company statements, utility bills and official correspondence to your residential address;
- asset and liability statements;
- documents gathered during the on-boarding process (including credit history, background vetting information);
- information gathered through our monitoring of its IT systems, building access records and CCTV recording when you attend meetings in person at our offices;
- passport, national identity card, driving licence, power of attorney and relevant contact information of your lawyers, accountants, advisers, agents, attorneys or other representatives (including their name, address, telephone number(s) and e-mail address(s));

- due diligence materials (including reports, photographs, valuations and analysis) relating to your property, assets, finances or creditworthiness for the purposes of credit analysis, consideration and approval; transaction structuring, processing and administration/management; and
- Personal Data which you otherwise voluntarily provide, for example when corresponding in writing (including via email or other electronic means), in meetings or during phone conversations or entered into any of our websites.

The majority of the Personal Data provided by you is mandatory in order for us to administer the client relationship and perform our obligations under our contract(s) with you and/or comply with statutory requirements relating to making or receiving payments, sanctions, immigration or taxation. Failure to provide mandatory Personal Data may affect our ability to accomplish the purposes stated in this privacy notice and potentially affect your ongoing client relationship with us.

Where permitted by law, we may process information about criminal convictions or offences and alleged offences for specific and limited activities and purposes, such as to perform checks to prevent and detect crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions. It may involve investigating and gathering intelligence on suspected financial crimes, fraud and threats and sharing data between Exepay Limited and with law enforcement and regulatory bodies.

The list set out above is not exhaustive, and there may be other Personal Data which we collect, store and use in the context of the client relationship.

4 How we obtain information

The majority of the Personal Data which we process will be collected directly from you. Your information is made up of all the financial and personal information we collect and hold about you/your business and the proprietors, officers and beneficial owners of that business and your transactions. It includes:

- information you give us;
- information that we receive from third parties – including third parties who we provide services to you and us, credit reference, fraud prevention or government agencies and financial institutions (where permitted by law);
- information that we learn about you through our relationships with you and the way you operate your account/or services;
- information that we gather from the technology which you use to access our services (for example an IP address or telephone number) and how you use it; and
- information that we gather from publicly available sources, such as the press, the electoral register, company registers and online search engines.

5 Credit reference and fraud prevention agencies

5.1 General

Before we provide services, goods or financing to you, we undertake checks for the purposes of preventing fraud and money laundering, and to verify your identity. 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 prevent fraud and money laundering, and to verify your identity.

Details of the personal information that will be processed include, for example: name, address, date of birth, contact details, financial information, employment details, device identifiers including IP address details.

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 verify identity, in order to protect our business and to comply with laws that apply to us. Such processing is also a contractual requirement of the services or financing you have requested.

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

5.2 Automated Decisions

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 using the details above.

5.3 Consequences of Processing

If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services or financing you have requested, or to employ you, or we may stop providing existing services to you.

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, please contact us on the details above.

5.4 Data Transfers

Whenever fraud prevention agencies transfer your personal data outside of the European Economic Area, they impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the European Economic Area. They may also

require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.

6 How Do We Use Your Personal Data?

ExePay Limited uses your Personal Data for a variety of purposes in order to perform its obligations under the contracts between you and us to comply with legal obligations or otherwise in pursuit of its legitimate business interests.

7 Schedule of Purposes of Processing

We will only use and share your information where it is necessary for us to carry out our lawful business activities. We want to ensure that you fully understand how your information may be used. We have described the purposes for which your information may be used in detail below:

7.1 Contractual necessity

We may process your information where it is necessary to enter into a contract with you for the provision of our products or services or to perform our obligations under that contract. Please note that if you do not agree to provide us with the requested information, it may not be possible for us to continue to operate your account and/or provide products and services to you. This may include processing to:

- assess and process applications for products or services;
- provide and administer those products and services throughout your relationship with the company, including opening, setting up or closing your accounts or products; collecting and issuing all necessary documentation; executing your instructions; processing transactions, including transferring money between accounts; making payments to third parties; resolving any queries or discrepancies and administering any changes. Calls to our service centre
- and communications to our mobile and online helplines may be recorded and monitored for these purposes.
- manage and maintain our relationships with you and for ongoing customer service.
- administer any credit facilities or debts, including agreeing repayment options; and
- communicate with you about your account(s) or the products and services you receive from us.

7.2 Legal obligation

When you apply for a product or service (and throughout your relationship with us), we are required by law to collect and process certain personal information about you. Please note that if you do not agree to provide us with the requested information, it may not be possible for us to continue to operate your account and/or provide products and services to you.

This may include processing to:

- confirm your identity, including using biometric information and voice-recognition technology and other
- identification procedures, for example fingerprint verification;
- perform checks and monitor transactions and location data for the purpose of preventing and detecting crime and

- to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions. This may require us to process information about criminal convictions and offences,
- to investigate and gather intelligence on suspected financial crimes, fraud and threats and to share data with law enforcement and regulatory bodies;
- assess affordability and suitability of credit for initial credit applications and throughout the duration of the relationship, including analysing customer credit data for regulatory reporting;
- share data with other companies and third parties to help recover funds that have entered your account as a result of a misdirected payment by such a third party;
- share data with police, law enforcement, tax authorities or other government and fraud prevention agencies where we have a legal obligation, including reporting suspicious activity and complying with production and court orders;
- deliver mandatory communications to customers or communicating updates to product and service terms and conditions;
- investigate and resolve complaints;
- conduct investigations into breaches of conduct and corporate policies by our employees;
- manage contentious regulatory matters, investigations and litigation;
- perform assessments and analyse customer data for the purposes of managing, improving and fixing data quality;
- provide assurance that the company has effective processes to identify, manage, monitor and report the risks it is or might be exposed to;
- investigate and report on incidents or emergencies on the company's properties and premises;
- coordinate responses to business-disrupting incidents and to ensure facilities, systems and people are available to continue providing services.

7.3 Legitimate interests

We may process your information where it is in our legitimate interests do so as an organisation and without prejudicing your interests or fundamental rights and freedoms.

a) We may process your information in the day-to-day running of our business, to manage our business and financial affairs and to protect our customers, employees and property. It is in our interests to ensure that our processes and systems operate effectively and that we can continue operating as a business. This may include processing your information to:

- monitor, maintain and improve internal business processes, information and data, technology and communications solutions and services;
- ensure business continuity and disaster recovery and responding to information technology and business incidents and emergencies;
- ensure network and information security, including monitoring authorised users' access to our information technology for the purpose of preventing cyber-attacks, unauthorised use of our telecommunications systems and websites, prevention or detection of crime and protection of your personal data;
- provide assurance on the company's material risks and reporting to internal management and supervisory authorities on whether the company is managing them effectively;

- perform general, financial and regulatory accounting and reporting;
- protect our legal rights and interests;
- manage and monitor our properties (for example through CCTV) for the purpose of crime prevention and prosecution of offenders, for identifying accidents and incidents and emergency situations and for internal training; and
- enable a sale, reorganisation, transfer or other transaction relating to our business.

b) It is in our interest as a business to ensure that we provide you with the most appropriate products and services and that we continually develop and improve as an organisation. This may require processing your information to enable us to:

- identify new business opportunities and to develop enquiries and leads into applications or proposals for new business and to develop our relationship with you;
- send you relevant marketing. We may show or send you marketing material online (on our own and other websites including social media platforms), in our app, or by email, SMS or post;
- understand our customers' actions, behaviour, preferences, expectations, feedback and financial history in order to improve our products and services, develop new products and services, and to improve the relevance of offers of products and services by the company;
- monitor the performance and effectiveness of products and services;
- assess the quality of our customer services and to provide staff training. Calls to our service centres and communications to our mobile and online helplines may be recorded and monitored for these purposes;
- perform analysis on customer complaints for the purposes of preventing errors and process failures and rectifying negative impacts on customers;
- compensate customers for loss, inconvenience or distress as a result of services, process or regulatory failures;
- identify our customers' use of third-party products and services in order to facilitate the uses of customer information detailed above; and
- combine your information with third-party data, such as economic data in order to understand customers' needs better and improve our services.

c) We may perform data analysis, data matching and profiling to support decision-making with regards to the activities mentioned above. It may also involve sharing information with third parties who provide a service to us.

d) It is in our interest as a business to manage our risk and to determine what products and services we can offer and the terms of those products and services. It is also in our interest to protect our business by preventing financial crime. This may include processing your information to:

- carry out financial and credit risk assessments;
- manage and take decisions about your accounts;
- carry out checks (in addition to statutory requirements) on customers and potential customers, business partners and associated persons, including performing adverse

media checks, screening against external databases and sanctions lists and establishing connections to politically exposed persons;

- share data with credit reference, fraud prevention agencies and law enforcement agencies;
- trace debtors and recovering outstanding debt;
- for risk reporting and risk management.

Application decisions may be taken based on solely automated checks of information from credit reference agencies and internal records. For more information on how we access and use information from credit reference and fraud prevention agencies see Credit reference and fraud prevention agencies in this document.

Again, these lists are not exhaustive, and we may undertake additional processing of Personal Data in line with the purposes set out above.

We will update this privacy notice from time to time to reflect any notable changes in the purposes for which it processes your Personal Data.

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 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.

8 Marketing information

Unless you have told us that you do not want to hear from us, we will send you relevant marketing information (including details of other products or services provided by us, companies which we believe may be of interest to you), by mail, phone, email, text and other forms of electronic communication. If you change your mind about how you would like us to contact you or you no longer wish to receive this information, you can tell us at any time by contacting us in writing at Info@exepay.co.uk.

9 Transferring information overseas

We will share client Personal Data with third parties located outside of the EEA from time to time for the purposes set out in this Privacy Notice. We may transfer your information to organisations in other countries on the basis that anyone to whom we pass it protects it in the same way we would and in accordance with applicable laws. In the event that we transfer information to countries outside of the European Economic Area (which includes countries in the European Union as well as Iceland, Liechtenstein and Norway), we will only do so where:

- the European Commission has decided that the country or the organisation we are sharing your information with will protect your information adequately;
- the transfer has been authorised by the relevant data protection authority; and/or

- we have entered into a contract with the organisation with which we are sharing your information (on terms approved by the European Commission) to ensure your information is adequately protected.

10 What Special Categories of Personal Data Do We Process?

Certain categories of data are considered “special categories” of Personal Data” and are subject to additional safeguards. We do not need your consent if we use special categories of your Personal Data in accordance with our written policy to carry out our legal obligations or exercise specific legal rights. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

11 When Do We Share Client Personal Data?

We will share client Personal Data with other parties only in limited circumstances and where this is necessary for the performance of the contract or to comply with a legal obligation, or otherwise in pursuit of its legitimate business interests as follows:

- where we have your permission;
- where required for your product or service;
- where we are required by law and by law enforcement agencies, judicial bodies, government entities, tax authorities or regulatory bodies around the world;
- with companys, financial institutions and payment services companies when making payment to or receiving payment from you;
- with background vetting specialists as part of the client on-boarding process and periodically thereafter to ensure Personal Data held is up to date;
- accountants, lawyers, notaries and other professional advisers when considering, structuring, documenting, concluding, terminating, varying, amending or renewing a particular transaction already in place with you;
- financiers, insurers, participants and sub-participants in order to consider and/or obtain funding, risk mitigation, insurance or other financial or risk support in relation to an agreement between you and us;
- IT service providers as part of routine testing, maintenance, development and improvement to the safety, security or functioning of our IT systems;
- with debt collection agencies;
- with credit reference and fraud prevention agencies;
- with third-party guarantors or other companies that provide you with benefits or services (such as insurance cover) associated with your product or service;
- where required for a proposed sale, reorganisation, transfer, financial arrangement, asset disposal or other transaction relating to our business and/or assets held by our business;
- send you relevant marketing information however we will not share your information with third parties for marketing purposes without your permission
- in anonymised form as part of statistics or other aggregated data shared with third parties; or

- where permitted by law, it is necessary for our legitimate interests or those of a third party, and it is not inconsistent with the purposes listed above.

In all cases, the client Personal Data is shared under the terms of a written agreement between us and the third party which includes appropriate security measures to protect the Personal Data in line with this privacy notice and our obligations. The third parties are permitted to use the Personal Data only for the purposes which we have identified, and not for their own purposes, and they are not permitted to further share the data without our express permission.

12 How Long Will My Personal Data Be Retained?

By providing you with products or services, we create records that contain your information. Records can be held on a variety of media (physical or electronic) and formats.

We manage our records to help us to serve our customers well (for example for operational reasons, such as dealing with any queries relating to your account) and to comply with legal and regulatory requirements. Records help us demonstrate that we are meeting our responsibilities and to keep as evidence of our business activities.

Retention periods for records are determined based on the type of record, the nature of the activity, product or service, the country in which the relevant company is located and the applicable local legal or regulatory requirements.

We may on exception retain your information for longer periods, particularly where we need to withhold destruction or disposal based on an order from the courts or an investigation by law enforcement agencies or our regulators. This is intended to make sure that we will be able to produce records as evidence, if they are needed.

Under some circumstances we may anonymise your Personal Data so that it can no longer be associated with you. We reserve the right to retain and use such anonymous data for any legitimate business purpose without further notice to you.

During the course of your client relationship with us we will review the Personal Data we hold in relation to you approximately every 12 months and any Personal Data which is no longer needed will be deleted. Following the termination of your client relationship with us we will typically retain data for the periods set out below:

General correspondence	6 years
Contractual documentation	6 years
Legal Deeds relating to transactions between you and us	12 years
Tax and accountancy records relating to your transactions	7 years
Background check results and related information	6 years
Financial and credit-related information	6 years

Personal data in archived e-mails or other electronic files	6 years
Forms of identification	6 years
CCTV	31 days

Retention periods may be changed from time to time based on business or legal and regulatory requirements.

13 How is my Personal Data secured?

We have put in place appropriate security measures to prevent your Personal Data from being accidentally lost, altered, disclosed, used or accessed in an unauthorised way. 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. Details of these measures may be obtained from Data Protection Officer (the “DPO”) by writing to us at info@exepay.co.uk.

Third parties will only process your Personal Data on our instructions and where they have agreed to treat the data confidentially and to keep it secure.

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

14 Your rights

We want to make sure that you are aware of your rights in relation to the personal data we process about you. We have described those rights and the circumstances in which they apply in the table below.

Rights	Description
Access – You have a right to get access to the personal information we hold about you.	For more information on how to get access to your information and the documents we need you to submit, please contact us at info@exepay.co.uk
Rectification – You have a right to rectification of inaccurate personal information and to update incomplete personal information.	<p>If you believe that any of the information that we hold about you is inaccurate, you have a right to request that we restrict the processing of that information and to rectify the inaccurate personal information.</p> <p>Please note that if you request us to restrict processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.</p>

<p>Erasure – You have a right to request that we delete your personal information.</p>	<p>You may request that we delete your personal information if you believe that:</p> <ul style="list-style-type: none"> • we no longer need to process your information for the purposes for which it was provided; • we have requested your permission to process your personal information and you wish to withdraw your consent; or • we are not using your information in a lawful manner. <p>Please note that if you request us to delete your information, we may have to suspend the operation of your account and/or the products and services we provide to you.</p>
<p>Restriction – You have a right to request us to restrict the processing of your personal information.</p>	<p>You may request us to restrict processing your personal information if you believe that:</p> <ul style="list-style-type: none"> • any of the information that we hold about you is inaccurate; • we no longer need to process your information for the purposes for which it was provided, but you require the information to establish, exercise or defend legal claims; or • we are not using your information in a lawful manner. <p>Please note that if you request us to restrict processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.</p>
<p>Portability – You have a right to data portability.</p>	<p>Where we have requested your permission to process your personal information or you have provided us with information for the purposes of entering into a contract with us, you have a right to receive the personal information you provided to us in a portable format. You may also request us to provide it directly to a third party, if technically feasible. We're not responsible for any such third party's use of your account information, which will be governed by their agreement with you and any privacy statement they provide to you. If you would like to request the personal information you provided to us in a portable format, please write to us at the details provided above.</p>

Marketing – You have a right to object to direct marketing.	You have a right to object at any time to processing of your personal information for direct marketing purposes, including profiling you for the purposes of direct marketing.
Withdraw consent – You have a right to withdraw your consent.	<p>Where we rely on your permission to process your personal information, you have a right to withdraw your consent at any time. We will always make it clear where we need your permission to undertake specific processing activities.</p> <p>Please note that if you withdraw your consent we may have to suspend the operation of your account and/or the products and services we provide to you.</p>
Lodge complaints – You have a right to lodge a complaint with the regulator.	If you wish to raise a complaint on how we have handled your personal information, you can contact our Data Protection Officer who will investigate the matter. We hope that we can address any concerns you may have, but you can always contact the Information Commissioner’s Office (ICO).

If you have any questions about these rights or you wish to exercise your rights of access you should set out your request to the DPO in writing to info@exepay.co.uk.

15 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 for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

16 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 the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it.

17 Where Can I get Further Information?

We have appointed the DPO to oversee compliance with this Notice. If you have any questions about this privacy notice or how we handle your Personal Data, please contact the DPO in writing to ExePay Limited at info@exepay.co.uk.

Finally, you have the right to raise any concerns about how your Personal Data is being processed with the Information Commissioner’s Office (ICO) by going to the ICO’s website:

<https://ico.org.uk/concerns/> or contacting the ICO on 0303 123 1113 or casework@ico.org.uk.