



Our Privacy Policy

Before we begin

This policy (Privacy Policy) applies to personal information held by E-pay International Limited as data controller, as described below. It explains what information we collect about you, how we'll use that information, who we'll share it with, the circumstances when we'll share it and what steps we'll take to make sure it stays private and secure. It continues to apply even if your agreement for payment services agreement or other products and services with us ends.

This Privacy Policy covers any products or services you have with us, including Virtual IBAN accounts, debit cards, payment gateway services and others. Sometimes we may need to provide you with separate or further information about specific products and services. This information will also apply.

Wherever we've said 'you', 'your' or 'Customer', this means you, any authorised person on your account, anyone who does your banking or deals with us for you (e.g. trustees or executors, attorneys under a Power of Attorney) and other related people (including authorised signatories, partners, members and trustees). A "User Account" is an account opened by E-pay International Limited that allows to view transaction data from the Customer's merchant account.

When we say 'we', we mean E-pay International Limited which acts as a data controller in respect of your personal data.

All of your data that are subject to this Privacy Policy are controlled and administered by E-Pay International Limited, registered in the United Kingdom with registration number: #10086951. E-Pay International LTD is an Authorised Payment Institution by the Financial Conduct Authority (FCA) of the United Kingdom, number 802210. E-Pay International Limited listed as a Visa Merchant Agent operating a PCI DSS Level 1 Certified Payment Gateway. E-Pay International Limited is VAT registered, VAT Number: GB310234074.

You need to accept all the provisions in this Policy when you sign up for the E-pay products and services. If you do not agree with anything in this Policy, then you may not register and/or use any of the products or services.

What information we collect

We'll only collect your information in line with relevant regulations and law. We may collect it from a range of sources and it may relate to any of our products or services you apply for, currently hold or have held in the past. We may also collect information about you when you interact with us, e.g. visit our websites, call us or ask about any of our products and services.

Some of it will come directly from you, e.g. when you provide ID to open an account. It can also come from your financial advisor or other sources you've asked us to obtain information from. We might also get some of it from publicly available sources.

The information we collect may include:

Information that you provide to us, e.g.:

- personal details, e.g. name, previous names, gender, date and place of birth;
- contact details, e.g. address, email address, landline and mobile numbers;
- information concerning your identity e.g. photo ID, passport information, National Insurance number, National ID card and nationality;
- user login and subscription data, e.g. login credentials for online banking;

- other information about you that you give us by filling in forms or by communicating with us, whether face-to-face, by phone, email, online, or otherwise;

Information we collect or generate about you, e.g.:

- your financial information and information about your relationship with us, including the products and services you hold, the channels you use and your ways of interacting with us, your payment history, transactions records, payments into your account and information concerning complaints and disputes;
- information we use to identify and authenticate you, e.g. your signature or additional information that we receive from external sources that we need for compliance purposes;
- information included in customer documentation, e.g. a record of advice that we may have given you;
- information about your device or the software you use, e.g. its IP address, technical specification and uniquely identifying data;
- cookies and similar technologies we use to recognize you, remember your preferences and tailor the content we provide to you—our cookie policy contains more details about how we use cookies and can be found at: https://www.monneo.com/cookie_policy;
- risk rating information, e.g., transactional behaviour and underwriting information;
- investigations data, e.g. due diligence checks, sanctions and anti-money laundering checks, external intelligence reports, content and metadata related to relevant exchanges of information between and among individuals and/or organisations, including emails, calls, etc.;
- records of correspondence and other communications between us, including email, calls and instant messages;
- information that we need to support our regulatory obligations, e.g. information about transaction details, detection of any suspicious and unusual activity and information about parties connected to you or these activities.

Information we collect from other sources, e.g.:

- information you've asked us to collect for you, e.g. information about your accounts or holdings with other companies including transaction information;
- information from third party providers, e.g. information that helps us to combat fraud.

How we'll use your information

We'll only use your information where we have your consent or we have another lawful reason for using it. These reasons include where we:

- need to pursue our legitimate interests;
- need to process the information to enter into or carry out an agreement we have with you;
- need to process the information to comply with a legal obligation;
- believe the use of your information as described is in the public interest, e.g. for the purpose of preventing or detecting crime;
- need to establish, exercise or defend our legal rights.

The reasons we use your information include to:

- deliver our products and services;
- carry out your instructions, e.g. to fulfil a payment request;
- manage our relationship with you, including (unless you tell us otherwise) telling you about products and services we think may be relevant for you;
- understand how you use your accounts and services;



- prevent or detect crime including fraud and financial crime, e.g. financing for terrorism and human trafficking;
- ensure security and business continuity;
- manage risk;
- provide online banking and other online product platforms;
- improve our products and services, including through analysing how you use them;
- protect our legal rights and comply with our legal obligations;
- correspond with solicitors, surveyors, conveyancers and third-party intermediaries;
- undertake system or product development and planning, insurance, audit and administrative purposes.

Further details of how we'll use your information can be found in the Appendix below.

How we make decisions about you

We may use automated systems to help us make decisions, e.g. when you apply for products and services, to carry out fraud and money laundering checks. We may use technology that helps us identify the level of risk involved in customer or account activity, e.g. for fraud or financial crime reasons, or to identify if someone else is using your card without your permission.

You may have a right to certain information about how we make these decisions. You may also have a right to request human intervention and to challenge the decision. More details can be found in the 'Your rights' section below.

Tracking or recording what you say or do

To help keep you and your money safe, we may record details of your interactions with us. We may record and keep track of conversations you have with us including phone calls, face-to-face meetings, letters, emails, and any other kinds of communication. We may use these recordings to check your instructions to us, assess, analyse and improve our service, train our people, manage risk or to prevent and detect fraud and other crimes. We may also capture additional information about these interactions, e.g. telephone numbers that you call us from and information about the devices or software that you use. Our websites, and other digital products may track and record your interactions with them.

Compliance with laws and regulatory compliance obligations

We'll use your information to meet our compliance obligations, to comply with other laws and regulations and to share with regulators and other authorities that E-pay is subject to. This may include using it to help detect or prevent crime (including terrorism financing, money laundering and other financial crimes). We'll only do this on the basis that it's needed to comply with a legal obligation, it's in our legitimate interests and that of others, or to prevent or detect unlawful acts.

Who we might share your information with

We may share your information with others where lawful to do so including where we or they:

- need to in order to provide you with products or services you've requested, e.g. fulfilling a payment request;
- need to in order to administer your claim;
- have a public or legal duty to do so, e.g. to assist with detecting and preventing fraud, tax evasion and financial crime;
- need to in connection with regulatory reporting, litigation or asserting or defending legal rights and interests;
- have a legitimate business reason for doing so, e.g. to manage risk, verify your identity, enable another company to provide you with services you've requested, or assess your suitability for products and services;
- have asked you for your permission to share it, and you've agreed.

We may share your information for these purposes with others including:

- people you make payments to and receive payments from;

E-Pay International LTD /Monneo | 61-63 Crockhamwell Road | Reading | United Kingdom | RG5 3JP
FCA: 802210 | Company: 10086951
www.monneo.com

- your beneficiaries, intermediaries, correspondent and agent banks, clearing houses and clearing or settlement systems;
- other financial institutions, tax authorities, payment service providers and debt recovery agents;
- any entity that has an interest in the products or services that we provide to you, including if they take on the risk related to them;
- any people or companies where required in connection with potential or actual corporate restructuring, merger, acquisition or takeover, including any transfer or potential transfer of any of our rights or duties under our agreement with you;
- law enforcement, government, courts, dispute resolution bodies, our regulators, auditors and any party appointed or requested by our regulators to carry out investigations or audits of our activities;
- other parties involved in any disputes, including disputed transactions;
- fraud prevention agencies who'll also use it to detect and prevent fraud and other financial crime and to verify your identity;
- anyone who provides instructions or operates any of your accounts on your behalf, e.g. Power of Attorney, solicitors, intermediaries, etc;
- anybody else that we've been instructed to share your information with by either you, or anybody else who provides instructions or operates any of your accounts on your behalf;
- our card processing supplier(s) to carry out fraud and risk checks, process your payments, issue and manage your card.

How long we'll keep your information

Your personal and business information are stored as long as it is necessary to duly perform E-pay services to you and other obligations resulting from the binding agreements and as long as it is required by the applicable law.

This enables us to comply with legal and regulatory requirements or use it where we need to for our legitimate purposes such as managing your account and dealing with any disputes or concerns that may arise.

If we don't need to retain information for any longer, we may destroy, delete or anonymise it.

Your rights

You have a number of rights in relation to the information that we hold about you. These rights include:

- the right to access information we hold about you and to obtain information about how we process it;
- in some circumstances, the right to withdraw your consent to our processing of your information, which you can do at any time. We may continue to process your information if we have another legitimate reason for doing so;
- in some circumstances, the right to receive certain information you have provided to us in an electronic format and/or request that we transmit it to a third party;
- the right to request that we rectify your information if it's inaccurate or incomplete;
- in some circumstances, the right to request that we erase your information. We may continue to retain your information if we're entitled or required to retain it;
- the right to object to, and to request that we restrict, our processing of your information in some circumstances. Again, there may be situations where you object to, or ask us to restrict, our processing of your information but we're entitled to continue processing your information and/or to refuse that request.

You can exercise your rights by contacting us using the details set out in the 'More details about your information' section below. You also have a right to complain to the UK Information Commissioner's Office by visiting ico.org.uk, or to the data protection regulator in the country where you live or work.



Fraud and Money Laundering

Fraud Prevention Agencies

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

The personal information you provide or which we've collected from you, or 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.

We'll process personal information such as your name, address, date of birth, contact details, financial information, and device identifiers e.g. IP address.

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 your identity. This enables us to protect our business and to comply with laws that apply to us. This processing is also a contractual requirement of any of our products or services you use.

Fraud prevention agencies can hold your personal data for different periods of time. If they're concerned about a possible fraud or money laundering risk, your data can be held by them for up to six years.

Consequences of Processing

If we, or a fraud prevention agency, have reason to believe there's a fraud or money laundering risk, we may refuse to provide the services you've requested. We may also stop providing existing products and 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 to you.

To find out more about our Fraud Prevention Agencies and how they manage your information, please visit each agency directly:

World-check One Thomson Reuters;

Comply Advantage.

What we need from you

You're responsible for making sure the information you give us is accurate and up to date, and you must tell us if anything changes as soon as possible. If you provide information for another, you'll need to direct them to this policy.

How we keep your information secure

We have implemented a wide range of measures in order to ensure the security and confidentiality of your data. These include physical, electronic and administrative safeguards such as firewalls, data encryption, SSL and other up-to-date technologies.



We enforce physical access controls to our buildings and files. In addition, only those employees who require personal information regarding our Customers to fulfill their employee's obligations gain access to such information.

We comply with applicable Payment Card Industry Data Security Standards (we obtained a PCI certificate) and endeavor to comply with all such rules at all times. Pursuant to such rules and regulations we are required to undergo periodic third-party assessments and periodic network scans to ensure that, among others, we have installed and maintain a firewall configuration to protect data; encrypt transmission of cardholder data and other sensitive information across public networks; do not use vendor-supplied defaults for system passwords and other security parameters; use and regularly update anti-virus software; develop and maintain secure systems and applications; restrict access to data to those with a business need-to-know; track and monitor all access to network resources and cardholder data; regularly test our security systems and processes; assign a unique ID to each person with computer access; restrict physical access to cardholder data.

It is extremely important that you do not disclose your account password to anyone. E-pay has designed internal security processes that encrypt Customer's password to protect it from being divulged or accessed by anyone other than you. Neither E-pay employees nor any of its contractors can obtain or access your password. Neither E-pay nor its contractors will ever ask you for your password via mail, email, telephone or in any other unsolicited manner. It is your responsibility to keep in secret your unique password and account information at all times.

We cannot guarantee the security of your data while it is being transmitted over the Internet and through servers that are out of our control. We do our best to protect your personal information but we cannot ensure or warrant the security of any information you transmit to our website or services. Therefore, if you make any data transmissions over the Internet, you are doing it at your own risk. Once we receive the data transmission, we make our best efforts to ensure its security and privacy on our systems.

More details about your information

If you have questions or concerns regarding this Privacy Policy, please do not hesitate to contact us either by using this link www.monneo.com/contact, an email: compliance@monneo.com or writing to us at:

E-Pay International LTD., address: 47 Red Lion Street, London, WC1R 4PF, United Kingdom

This Privacy Policy may be updated from time to time and the most recent version can be found at www.monneo.com/Privacy_Policy.

This policy was last updated in June 2019

Appendix—How we process your information

E-pay uses the information received from you or otherwise collected only in the scope that is necessary to operate, maintain, improve and provide E-pay products and services and all of the functions available on our websites and to allow us to duly perform our obligations resulting from binding agreements, in particular those regarding assisting in executing payment transactions. We also analyse all of the said information to determine the trends and preferences of our Customers, improve our websites and services, inclusive of creating new features and functionality.

We'll use your information for purposes including:

- **To deliver our products and services:** administer your accounts, or process your transactions. We'll do this in order to perform our contract with you; i.e.
 - Information received or collected by E-pay in the process of opening of an account. Such information may be used by E-pay in order to: (i) evaluate your eligibility for an account; (ii) duly provide services to you; (iv) verify your identity; (v) manage and administer your use of the services; (vi) comply with any applicable legislation requiring E-pay to obtain, verify and record such information, (vii) inform you, subject to obtaining your prior consent, of competitions, promotions and special offers from us and/or our partners.
 - Information received upon subscription for certain services, competitions or functions on our websites. Such information is used in the scope necessary to: (i) provide you such services or functions, admit to promotions and competitions, etc.; (ii) contact you.
 - Information provided by merchants (our users). Such information is used for the purpose of: (i) facilitating payment transactions initiated by you and submitted to us by the Merchant, in the course of providing E-pay services to our merchant; (ii) complying with any binding law or the rules and regulations of the respective card organizations or other payment entities (e.g. Visa, MasterCard).
 - Information provided by you together with your inquiry. The information submitted by you via an inquiry may be used by E-pay to: (i) respond to your inquiries; (ii) contact you; (iii) inform you of services of E-pay or its partners that may be of use to you, (iv) taking action to conclude a contract.
 - Information obtained through "cookies" and browsing the websites. We may use information obtained in this manner to: (i) remember your information so that you will not have to re-enter it during your visit or the next time you access the websites; (ii) monitor websites usage trends and generating statistical information; (iii) track your entries, submissions, and status in any promotions or other activities in connection with your usage of the websites or services; (iv) manage the websites or improve their performance, (v) comply with certain laws, regulations, and card association rules and regulations
- **Payment service provider's operations support:** we'll use your information to enable the provision and function of our services in line with regulation, laws and customer rights and interests, e.g. complaints management and exit management. The lawful reasons for processing these are legitimate interest, legal obligation and in order to perform our contract with you;
- **To prevent and detect crime including, e.g. fraud, terrorist financing and money laundering:** this will include monitoring, mitigation and risk management, carrying out customer due diligence, name screening, transaction screening and customer risk identification. We do this to comply with our legal obligations and because it's in our legitimate interest. We may share your information with relevant agencies, law enforcement and other third parties where the law allows us to for the purpose of preventing or detecting crime. Additionally, we and other financial institutions may take steps to help prevent financial crime and manage risk.

We'll do this because we have a legitimate interest, a legal obligation to prevent or detect crime or it's in the public interest. We may be required to use your information to do this, even if you've asked us to stop using your information. That could include (among other things):

- screening, intercepting and investigating any payments, instructions or communications you send or receive (including drawdown requests and application forms);
 - investigating who you're paying or who's paying you, e.g. checks on payments into and out of your account and other parties related to those payments;
 - passing information to relevant agencies if we think you've given us false or inaccurate information, or we suspect criminal activity;
 - checking whether the people or organisations you're paying or receiving payments from are who they say they are, and aren't subject to any sanctions.
- **Online Banking and other online product platforms:** we'll use your information to allow us to provide you with access to E-pay online platforms. The platform may allow you to directly or indirectly communicate with us, such as using Online



Banking, or applying for products and services online. The lawful basis for using your information for this purpose is to perform our contract with you or that processing for this purpose is in our legitimate interest;

- **Protecting our legal rights:** we may need to use your information to protect our legal rights, e.g. in the case of defending or the protection of legal rights and interests (e.g. collecting money owed, enforcing or protecting our security or defending rights of intellectual property); court action; managing complaints or disputes; in the event of a restructuring of companies or other mergers or acquisition. We'd do this on the basis that it's in our legitimate interest