Privacy Policy
Overview and Scope

Velapay respects your privacy and protecting your information is paramount. As a financial services provider, we take data security extremely seriously and we make sure we have appropriate security measures in place to prevent your personal data from being accidentally lost and from unauthorised use and access. Please read this Privacy Policy carefully as it explains our practices regarding your personal data and how we will treat it. This Privacy Policy (together with our Cookie Policy) sets out the basis on which any personal data will be processed by us.

For the purpose of the applicable data protection legislation (meaning, prior to 25 May 2018 the Data Protection Act 1998 and from 25 May 2018 the General Data Protection Regulation and any legislation which implements it) (the "Data Protection Legislation"), the data controller is Velapay of 36-38 Cornhill, London, EC3V 3NG.

Our data controller registration number is ZB283390. You can check our registration on the Data Protection Public Register by visiting https://www.ico.org.uk/esdwebpages/search. References in this Privacy Policy and on our website to "we", "our" or "us" are references to Velapay. References to "you" and "your" means each natural or legal person who interacts with us, uses our website or the products and services we provide.

Information we collect and process about you:

We may collect and process the following personal data about you:
Information you give us. You may give us information about you when you register with our website www.velapay.co.uk (our website) or by communicating with us by phone, email or otherwise. This also includes information you provide when you subscribe to our services, provide us with feedback, participate in surveys, and when you report a problem with our website. The information you give us may include your name, address, email address, phone number, date of birth, identity documents, username (or similar identifier), job title and company information. If you engage with us through social media then this may also include your social media contact details, such as your LinkedIn address or Twitter username. Information we collect about you when you communicate with us by phone, email, post, in person or otherwise, and when you use our products and services. We collect engagement metric information such as information about how, when and how often you contacted us, how, when and how often you responded to communications from us and how and when you use our products and services.

Information we collect about you if you use our website or interact with us over the internet, including via social media:

Each time you visit our website or interact with us we may automatically collect the following information: (a) technical information, including the Internet protocol (IP) address used to connect your device to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform; (b) information about your visit, including the full Uniform Resource Locators (URL)

clickstream to, through and from our website (including date and time); products you viewed or searched for; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page and any phone number used to call our customer service number.

Information we collect about you from publicly available sources:

This may include information available from social media (depending on your settings and the applicable privacy policies), including social media engagement metrics such as numbers of connections, followers and clicks, and information from resources such as Companies House.
Information we receive from other sources. We may receive further information about you if you use any of the services we provide. We work closely with third parties (including, for example, business partners, service providers, and identity verification providers) and may receive information about you from them. We may combine information we receive from these other sources with information you give to us and information we collect about you. We may monitor or record telephone conversations or other communications between you and us and keep recordings or transcripts of them and, if you contact us, we may keep a record or copy of that correspondence.
We also collect, use and share aggregated data such as statistical or demographic data. Aggregated data may be derived from your personal data, but it is not considered personal data under the Data Protection Legislation as it does not directly or indirectly identify you. If at any time we do combine any aggregated data with your personal data so that it can identify you, we treat the combined data as personal data, which we will use and process in accordance with this Privacy Policy.

Cookies:

We and our service providers collect information about your use of our website from cookies. For information about our use of cookies and how to decline them please read our Cookies Policy.

Purposes and legal basis for using your personal data:

Where you have requested that we provide a specific product or service to you, or you otherwise make use of those products or services, we will process your personal data in order to perform our contract with you and provide that product or service.
We also use the personal data we hold about you to pursue our legitimate interests in providing and marketing our products and services to you, improving our website, services and interactions with you and other users of our products and services in the following ways:

- administer your account and relationship with us and, communicate with you by telephone, mail, email, text (SMS) message, instant messaging or other electronic means;

- verify your identity as part of our identity authentication process and to prevent, detect and prosecute fraud and crime and comply with legal or regulatory; requirements;
- provide you with information about the products and services that you request from us;
- provide you with information about other products and services we offer that are similar to those that you have already purchased or enquired about;
- provide you with information about products or services we feel may interest you or be best for you;
- your data may be shared with product or service providers to validate if you are an existing customer (which may affect whether you can be accepted for one of their products) or for fraud prevention purposes. The product or service provider does not have permission to use these data for any other purpose including marketing.
- notify you about changes to our services;
- ensure that content from our website is presented in the most effective manner for you and your device;
- aggregate it on an anonymous basis with other data for data analytical and reporting purposes;
- to administer our website and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- to build up a picture of your interests so that you don't miss information relevant to you when you visit our website;
- to improve the service we offer you and to try and ensure that you get the best from our website in the short term, for example by providing you with relevant search results;
- to improve the service we offer you and to try and ensure that you get the best from our website over the longer term, for example by understanding how you and other users interact with our website
- to allow you to participate in interactive features of our service when you choose to do so;
- as part of our efforts to keep our website safe and secure;
- to measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising to you;
- to make suggestions and recommendations (both through the website and other channels, such as email) to you and others about products or services that we think may interest you or them based on your and their usage patterns both on our website and in relation to our communications with you and them on other channels (such as email);
- for training and quality purposes;
- to check any instructions you give to us and for the purposes of investigating any complaint you may make, or as evidence in any dispute or anticipated disputes between you and us.
- In some cases, we may also use the personal data we hold about you to comply with our legal obligations, or enter into or perform a contract with you.
- Where we have your consent, we may also send you direct marketing communications (for example, by email). You can withdraw this consent at any time as described in section 5 below.

Who your data can be disclosed to:

- Disclosure of your data to others may be necessary to ensure the smooth provision to you of the products, services and information you request. Your data may be disclosed to the other entities as described below.
- We may share your personal information with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries.
- We may share your information with selected third parties including:
    - Fraud prevention agencies, to prevent crime and trace those responsible;
    - Identity verification providers, to comply with legal or regulatory requirements;
    - Business partners, suppliers and sub-contractors for the performance of any contract we enter into with you;
    - Analytics and search engine providers that assist us in the improvement and optimisation of our website;
    - IT and software providers who supply us with our IT infrastructure for the provision of our services and administering our business (including our internal and external communications) and who also help us manage our customer and contact databases, customer relationships and marketing.

We may disclose your personal information to third parties if:

- we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets;
- Velapay or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets; and
- we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with you and other agreements; or to protect the rights, property, or safety of Velapay, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud and other crime prevention and detection.
- We have processes and systems that protect our customers and ourselves against fraud and other crimes. Customer information can be used to prevent crime and trace those responsible. We will share your personal information with fraud prevention agencies. If false or inaccurate information is provided and fraud is identified, details of this fraud will be passed to these agencies. Law enforcement agencies may access and use this information. Other organisations may also access and use this information to prevent fraud and money laundering, for example when checking details on applications for financial services, or checking details of job applicants and employees.
- We and other organisations may access and use the information recorded by fraud prevention agencies from other countries.
- We review all our relationships with third parties carefully so that we can be sure as possible that their practices match our own commitments to you relating to privacy and security. We also comply with the Data Protection Legislation in our dealings with these third parties to ensure that your information is appropriately protected.

Direct marketing and how you can change your preference:

- Where we have your consent we may send direct marketing communications to you, including by email, telephone, SMS or mail.
- Whenever you receive direct marketing from us you will be told how you can unsubscribe so that you no longer receive it. When we communicate with you via email you will also be given the opportunity to set or amend any preferences that you have indicated to us.
- You are also able at any time to withdraw any consent to receive marketing communications that you have given to us. You can do this by contacting us at info@velapay.co.uk or by writing to us at:

Velapay
International House,
36-38 Cornhill,
London,
EC3V 3NG

Please provide us with your full name, address and other contact details to enable us to find your records. Sometimes we may also need to contact you further to ask you for additional information so that we can comply with your request.

Where we store and transfer your data:

- Where we store your information ourselves it is stored on our secure servers in the European Economic Area (EEA). However, where we share your information with third parties this may involve transferring it to a country outside the EEA. This may include countries that do not have data protection laws which are as strong as those in the UK or the EEA. Where we do this we will take the steps required under the Data Protection Legislation to ensure that your information is appropriately protected. If you would like any further information about this then please contact us using the details in the Contact section below
- Unfortunately, the transmission of information via the Internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our website; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access, loss or damage.

How long we keep your information for:

- How long we keep your information will depend on the purpose for which we use it and so may vary. We will only retain your information for as long as is necessary for the purposes set out in this Privacy Policy and as is necessary to comply with our legal obligations. We do not keep more information than we need for a particular purpose.
- Where we have provided you with a product or service we will keep an archived record of your personal data for a period of up to 6 years after termination (unless a

longer period is prescribed by law) for the purposes of responding to legal disputes and legal or regulatory enquiries or investigations only, but will not use this data for any other purpose.

In order to ensure that we provide reliable and effective products and services, and to comply with our regulatory obligations, we regularly make back-up copies of our data. If we have provided any products or services to you then this will include your personal data. Where we delete your personal data from our systems, for whatever reason, then a copy may be retained in our data back-ups for a period of up to 90 days afterwards. These are kept securely and only accessed in order to delete old versions or in the event of an emergency which means we have to utilise a backup copy to reinstate data on our active systems. Where we have to do this we will work to ensure as soon as we reasonably can that the copy of the data that has been used to reinstate data on our active systems is updated to take account of any previous amendments and deletions regarding your personal data.

If you ask us to stop sending direct marketing communications to you (see section 5, above), we will keep the minimum amount of information necessary (such as your name and email address) to ensure that we are able to adhere to your request. We also routinely seek to minimise the amount of personal data we hold where any marketing contact is deemed inactive. We deem a contact to be inactive if we have not been able to identify any engagement (e.g. through opening an email or visiting our website) for a period of 12 months or if an email is not delivered due to a hard bounce. In such circumstances, we will anonymise all relevant data for aggregation purposes, with the exception of an email address. This does not affect your rights as set out in Section 5 and Section 9 of this Privacy Policy.

Third-party websites:

Our website may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Your rights:

- Under the Data Protection Legislation, you have certain rights in respect of the personal data we hold about you. These may include rights to: request a copy of the personal data that we hold, request that we correct personal data if it is inaccurate, request that we erase or block your personal data, and to object to our processing of your personal data. These rights are limited in some situations. For example, if we have a legal requirement or a compelling legitimate ground we may continue to process your data even where you request its deletion.
- If you would like to exercise any of these rights, please contact us using the details in the Contact section below.
- You also have the right to make a complaint if you feel your personal data has been mishandled. We would encourage you to contact us in the first instance but you are

also entitled to complain directly to the Information Commissioner's Office (ICO) (if you are in the UK), or to your local data protection authority (if you are outside the UK).

Managing Data transfer outside of the EEA (European Economic Area)

- Legal Basis for Transfer: Before transferring Personal Data outside the EEA, it's essential to establish a lawful basis for the transfer. This may include obtaining explicit consent from the data subjects, entering into data processing agreements with third-party recipients, or relying on other legal mechanisms permitted under GDPR, such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or approved certification mechanisms.

- Assessment of Adequacy: Assess the adequacy of data protection laws and regulations in the recipient country or jurisdiction. The GDPR permits transfers to countries that are deemed to provide an adequate level of data protection by the European Commission. If the recipient country is not considered adequate, additional safeguards must be implemented to ensure an equivalent level of protection.

- Implementing Safeguards: Implement appropriate safeguards to protect Personal Data during transit and upon arrival in the recipient country. This may involve incorporating SCCs or other contractual clauses into agreements with data recipients to ensure that they adhere to GDPR standards for data protection.

- Data Minimisation and Anonymisation: Minimise the amount of Personal Data transferred outside the EEA to only what is strictly necessary for the intended purpose.

- Security Measures: Implement robust security measures to safeguard Personal Data during transfer, including encryption, access controls, and secure transmission protocols (e.g., Secure Sockets Layer (SSL) or Transport Layer Security (TLS)).

- Due Diligence: Conduct due diligence on third-party recipients of Personal Data outside the EEA to ensure they have appropriate data protection measures in place. This may include assessing their privacy policies, security practices, and compliance with relevant regulatory requirements.

- Documentation and Record-Keeping: Maintain detailed documentation of all data transfers outside the EEA, including the legal basis for the transfer, safeguards implemented, and any relevant assessments or approvals obtained. This documentation is essential for demonstrating compliance with GDPR and may be subject to regulatory scrutiny.

- Monitoring and Review: Continuously monitor and review data transfer activities to ensure ongoing compliance with GDPR requirements. Regularly assess the

effectiveness of implemented safeguards and adjust them as necessary to address any changes in the regulatory landscape or business operations.

Changes to our privacy policy:

Any changes we may make to our Privacy Policy in the future will be posted on this page and, where we consider it appropriate, notified to you by email. Please check back frequently to see any updates or changes to our Privacy Policy.

Contact:

Questions, comments and requests regarding this Privacy Policy should be addressed to support@velapay.co.uk. Alternatively, you can write to us at:

Velapay
International House,
36-38 Cornhill,
London,
EC3V 3NG