OpenPayd Privacy Notice

About

The OpenPayd services will be provided to you by one of the following entities, depending on the entity you contract with, as set out in your Pricing Agreement:

SettleGo Solutions Limited, trading as OpenPayd is:

contactable by email at operations@openpayd.com, phone at +44 (0) 208 194 5050 or post at OpenPayd, The Bower, 207-211 Old Street, London, EC1V 9NR

incorporated in England and Wales (Company registration number 09570221), with registered office at The Bower, 207-211 Old Street, London, England, EC1V 9NR

registered with the Information Commissioner (No. ZA548790)

authorised by the Financial Conduct Authority under the Electronic Money Regulations 2011 (with firm reference number 900483) for the issuing of electronic money

OpenPayd Financial Services Malta Limited, trading as OpenPayd is:

contactable by email at operations@openpayd.com, phone at +365 2703 4054 or post at OpenPayd, 122 – 123 Pangea, Level 5 , Triq San Gorg, St. Julians STJ 3204, Malta

incorporated in Malta (Company registration number C75880), with registered office at 122 – 123 Pangea, Level 5, Triq San Gorg, St. Julians STJ 3204, Malta

authorised by the Malta Financial Services Authority as a financial institution licenced to issue electronic money and undertake payment services under the Financial Institutions Act, Chapter 376 of the laws of Malta

OpenPayd Financial Services Malta Limited, French Branch, trading as OpenPayd is:

contactable by email at operations@openpayd.com, or post at OpenPayd Financial Services Malta, French Branch, 49 Boulevard de Courcelles 75008 Paris, France

established in France by virtue of a Branch which is registered with the Paris commercial and companies register (RCS) under number 914 212 360 and whose registered office is located at 49 Boulevard de Courcelles 75008 Paris, France

authorised by the Malta Financial Services Authority which is located at Triq l-Imdina, Zone 1, Central Business District, Birkirkara, CBD 1010, Malta (www.mfsa.mt) as a financial institution licensed to issue electronic money and undertake payment services under the Financial Institutions Act, Chapter 376 of the laws of Malta

authorised and supervised by the Malta Financial Services Authority in Malta and supervised by the ACPR (Autorité de contrôle prudentiel et de resolution) in France which is located at 4 place de Budapest, 75009 PARIS cedex 9, France (www.acpr.banque-france.fr) to issue electronic money and undertake payment services in France under the freedom of establishment

OP Digital Services Limited, trading as OpenPayd is:

contactable by email at support@openpayd.com, phone at +33 1 89 71 17 96 or post at 122 – 123 Pangea, Level 5, Triq San Gorg, St. Julians STJ 3204, Malta

incorporated in Malta (Company registration number C110012), with registered office at 122 – 123 Pangea, Level 5, Triq San Gorg, St. Julians STJ 3204, Malta

authorised by the Malta Financial Services Authority under the Virtual Financial Assets Act as a VFA Service Provider, facilitating a range of regulated crypto-asset services, including the provision of custodial or nominee services, dealing on its own account, and the execution of orders on behalf of clients

OpenPayd Canada Inc., trading as OpenPayd is:

contactable by email at support@openpayd.com, phone at +1 289 803 0972 or post at 333 Bay Street, Suite 2400, Toronto, Ontario, Canada, M5H 2T6

incorporated in Canada (Company registration number 1159152-5), with registered office at 333 Bay Street, Suite 2400, Toronto, Ontario, Canada, M5H 2T6

registered with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as a money services business (registration number M19528814)

Privacy Notice

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

KEEPING YOUR DATA SAFE

We are committed to protecting your personal data and handling it securely and in full compliance with our legal obligations. Depending on the context, this privacy notice applies to visitors to our website; existing and prospective corporate clients of OpenPayd; or their end-users (both businesses and individuals) whose personal data is processed by OpenPayd.

This privacy notice explains in detail the purposes for which we process personal data, the parties with whom we may share it, the rights you have in relation to your personal data, and other information we believe is important for you to understand. If you represent an organisation that uses or intends to use our services, as defined in the relevant Terms, as a corporate client of OpenPayd, you are responsible for ensuring that your End Users are informed of the use of OpenPayd and have access to this privacy notice.

OpenPayd operates through a number of different legal entities, details of which can be found here. When we refer to “OpenPayd”, “we”, “us”, or “our” in this privacy notice, we mean the relevant OpenPayd entity that is responsible for the processing of your personal data. OpenPayd Holdings Limited is responsible for the operation of our website and, unless we notify you otherwise, acts as the data controller in relation to your use of it.

HOW WE COLLECT PERSONAL DATA AND OUR ROLE

Depending on the context and the specific processing activity, we act either as a data controller or as a data processor, in accordance with the applicable data protection law.

Where we act as a Data Controller

We act as an independent data controller where we determine the purposes and means of processing personal data, including where processing is required to comply with our own legal and regulatory obligations.

Direct interactions

Where you interact with us directly, we act as a data controller. You may provide us with your personal data by filling in forms or by corresponding with us by post, phone, email, via our website, or through the OpenPayd Platform. This includes personal data you provide when you:

- apply for, or use, our products or services;
- submit forms on our website or platform;
- subscribe to newsletters or other publications;
- request marketing communications;
- enter a competition, promotion, or survey; or
- provide feedback; or
- otherwise contact us.

Corporate client onboarding

We act as a data controller when processing personal data collected during the onboarding of our corporate clients, including for Know Your Business (KYB), anti-money laundering (AML), counter-terrorist financing (CTF), sanctions screening, transaction monitoring and other regulatory compliance purposes.

This may include personal data obtained directly from the corporate client or from publicly available sources (such as company registries and official databases), where such processing is necessary to meet our legal and regulatory obligations.

Automated technologies

When you use our website or the OpenPayd Platform, we act as a data controller in relation to the collection of Technical Data through cookies, server logs, and similar technologies. Further details are set out in our Cookies Policy.

Where we act as a data processor

We act as a data processor where we process personal data of End Users on behalf of our corporate clients and in accordance with their documented instructions, for the purpose of providing our services.

Provision of payment services and named virtual IBANs

In the context of allocating named virtual IBANs to our corporate client's End Users, we process personal data relating to End Users on behalf of the relevant corporate client.

In these circumstances:

- the corporate client acts as the data controller; and
- we act as a data processor, processing personal data solely for the purposes of delivering our services.

Personal data processed in this context may be received from:

- the corporate client, where end-user data is provided to us to enable allocation and management of named virtual IBANs; and
- the End User's sending bank, where personal data is transmitted to us in connection with payment transactions.

The merchant you choose to do business with may further share your personal data with third parties (such as additional third-party service providers other than OpenPayd). Please review their privacy policy for more information about how they collect, use, process, and handle your Personal Data.

Processing as an independent controller in regulated contexts

Notwithstanding the above, we act as an independent data controller in relation to any personal data we are required to process in order to comply with applicable laws and regulatory requirements, including AML, CTF, fraud prevention, transaction monitoring, and sanctions obligations.

In such cases, our processing is carried out independently of the corporate client's instructions and is based on our own legal obligations under applicable financial services and AML legislation.

CATEGORIES OF PERSONAL DATA WE COLLECT

Our collection and use of Personal Data differs based on whether you are an End User, Representative, or Website Visitor, and the specific service that you are using:

Category of Personal Data	Description
Contact Data	Address, email address, telephone numbers and other contact details
Identity Data	Name, surname, username or similar identifier, marital status, title, date of birth, identification number, nationality, place of birth, tax registration number, and role or position.

Transaction Data	Data collected or used in relation to transactions, including your name, address, bank and payment details, transaction amount, payment status information, and payment reference details.
KYC/ KYB Information	Information required to verify identity and comply with regulatory obligations, which may include: • a copy of an identity document (e.g. passport or driving licence) and a photograph • proof of address (e.g. utility bill or bank statement) • business information, such as (where required) certificate of incorporation, memorandum and articles of association, share certificates, register of directors, authorised signatory lists, position and identification documents of shareholders, directors and authorised signatories • politically exposed person (PEP) declarations • images in photo or video form and facial scan data extracted from such images (biometric data) for identity verification and fraud prevention during onboarding • information about other individuals associated with an account (e.g. directors, shareholders or authorised signatories), as required to comply with KYC, KYB, AML and other legal obligations and to support fraud monitoring • Sensitive or special categories of personal data, such as biometric data for facial recognition
Enhanced Due Diligence (EDD) Information	Information collected to verify the source of funds or source of wealth, or to carry out enhanced due diligence where required by law. The specific information requested will depend on the circumstances and will be communicated at the time of collection and might include sensitive or special categories of personal data.
Sanctions Screening and Transaction Monitoring Data	Information relating to corporate clients and their End Users, such as name, address, date of birth, transaction data, payment information, potential sanctions matches, and information or results arising from transaction monitoring and suspicious activity checks (e.g. transaction volumes or patterns).
Technical Data	Internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology used to access our website, the OpenPayd Platform or other OpenPayd applications.
Usage Data	Information about how you use our website, platform, products and services.
Marketing and Communications Data	Contact details such as name, business email address, job title, phone number and country, as well as your preferences for receiving marketing communications from us or third parties and your communication preferences.
Voluntary Information	Personal data voluntarily provided by you when communicating with us (for example by phone, email, post or social media) or by participating in competitions, promotions or surveys.
Aggregated Data	Statistical or aggregated data derived from personal data that does not directly or indirectly identify you. Aggregated Data is not considered personal data unless it is combined with other data in a way that enables identification, in which case it is treated as personal data in accordance with this privacy notice.

SPECIAL CATEGORIES AND SENSITIVE PERSONAL DATA

Some types of personal data are considered special categories or sensitive personal data under applicable data protection laws and therefore require a higher level of protection. Where we process such data, we apply enhanced technical and organisational safeguards.

Special categories of personal data may include information about an individual's race or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, health, sex life or sexual orientation, and genetic or biometric data.

Under applicable US privacy laws, sensitive personal data may include government-issued identification numbers, financial account information, precise geolocation data, biometric identifiers, account login credentials, and certain information relating to nationality, health, or children.

Where OpenPayd processes personal data that includes special categories of personal data or personal data, OpenPayd ensures that the applicable conditions under data protection laws are satisfied. In particular, OpenPayd ensures that:

- one or more of the conditions set out in Article 9(2) of the EU/UK GDPR applies, including where the processing is necessary for reasons of substantial public interest; and/or
- where relevant, the conditions set out in Article 10 of the EU/UK GDPR are met.

Processing of Biometric data for identity verification

Where OpenPayd processes biometric data as part of its identity verification procedures, the following lawful bases and conditions apply:

General lawful basis for processing

Article 6(1)(c) of the EU/UK GDPR: the processing is necessary for compliance with a legal obligation to which OpenPayd is subject, including obligations arising under applicable UK and EU anti-money laundering and counter-terrorist financing (AML/CTF) legislation.

Specific condition for processing special category data

Article 9(2)(g) of the EU/UK GDPR: the processing is necessary for reasons of substantial public interest, on the basis of Union law, Member State law, and/or UK law.

Applicable substantial public interest condition Preventing and detecting fraud and other unlawful or illicit activity.

US Biometric privacy laws

In addition, certain US state biometric privacy laws may regulate the collection, use, storage, and disclosure of biometric identifiers and biometric information, including, without limitation:

- the Illinois Biometric Information Privacy Act (BIPA) (740 ILCS 14);
- the Texas Capture or Use of Biometric Identifier Act (CUBI) (Texas Business and Commerce Code, Chapter 503); and
- the Washington Biometric Identifiers law (Revised Code of Washington, Chapter 19.375) (together, the "US Biometric Privacy Laws").

In order to verify you as a Representative, we may use third-party technology from Sum and Substance Ltd. (hereinafter "SumSub") to collect personal data and/or information from or about you, including biometric information and biometric identifiers such as a liveness check (collectively with Biometric Information, the

"Personal Data"). Specifically, we and/or SumSub will ask you to take a selfie through the SumSub application. SumSub will then scan and map your facial features in comparison with the picture on your government-issued identification for the purposes of OpenPayd's identity verification process. OpenPayd and SumSub may use your Personal Data, in each case as further described in this Notice and/or SumSub's Privacy Notice.

By tapping on the "**Continue**" button or otherwise continuing the verification procedure, and providing us with your Personal Data, including your Biometric Information, you consent to OpenPayd's and SumSub's collection, storage, retention, use and disclosure of your such information for the purposes, consistent with this Notice.

By tapping on the "Continue" button providing SumSub with your Personal Data, including your Biometric Information, you agree you have read, understand and accept Sumsub's Privacy Notice.

LEGAL BASES FOR PROCESSING PERSONAL DATA

We rely upon a number of legal grounds to enable our use of your personal data. In short, we use personal data to facilitate the business relationshipswe have with corporate clients, to comply with our financial regulatory and other legal obligations, and to pursue our legitimate business interests. We also use personal data to complete transactions and to provide the services to our corporate clients.

The table below provides a detailed overview of why and how we use your personal data.

Data Subjects	Purpose / Activity	Type of Data	Legal Bases for Processing
End users	• Provision of payment services to our corporate client • Depending on how the corporate client has integrated services we receive your personal data directly from you, corporate client, including from your sending bank when you make payments • Fraud prevention	• Identity data • Transaction data • Sanctions Screening and Transaction Monitoring Data	• Legal obligation • Legitimate interest
Representatives of a potential or existing corporate client	• Client onboarding and verification, include the processing of biometric data • Fraud prevention • Communications • Advertising	• Identity Data • Contact data • Usage data • Marketing and communications data • Enhanced Due Diligence (EDD) Information • KYC/ KYB Information (which may include biometric data for facial recognition) • Technical data	• Legal obligation • Legitimate interest • Consent (where required by law for processing of biometric data)
Representatives of banking partners or third-party service providers	• To enter a contract • To perform a third-party due diligence • To manage our business relationship	• Identity data • Contact data • Marketing and Communications information • KYC Information • EDD Information	• Legal obligation • Legitimate interest

Website Visitors	• Communications • Advertising	• Identity Data • Contact data • Usage data • Marketing and communications data • Voluntary data	• Consent • Legitimate interest

IF YOU DO NOT PROVIDE YOUR DATA

Some personal data is required for us to meet our legal obligations and provide our services. If you do not provide this information, we may be unable to offer or continue to provide the OpenPayd platform, products, or services.

RECIPIENTS AND SHARING OF PERSONAL DATA

We do not sell your personal data. However, we may share your personal data in the manner and for the purposes described below, where necessary to provide our services, manage our business, comply with applicable laws and regulations, or with your consent.

Category of recipient	Who we share data with	Purpose of sharing
OpenPayd Group	OpenPayd operates as a group of companies. We may share personal data within the OpenPayd Group.	For purposes such as onboarding, customer support and operations, sanctions screening, transaction monitoring, platform development and IT support.
Banking and payment network providers	Banks, financial institutions, acquirers, alternative payment providers, payment schemes, account information service providers, payment gateways, etc.	To enable the execution of payments, and other related payment services. This may include sharing personal data, including KYC/KYB and enhanced due diligence (EDD) information, to meet regulatory, compliance and fraud-prevention obligations
Service providers	Third-party service providers providing IT infrastructure and hosting, cloud storage, biometric verification, transaction monitoring and risk management services, analytics, marketing, customer relationship management systems, customer support tools, chatbots, document repositories, security services, tax reporting services, and payment processing services	To operate, secure, support, analyse, and improve our services. These providers act as processors or sub-processors under our instructions, or as independent controllers where applicable, and are contractually required to protect personal data and use it only for permitted purposes
Fraud prevention agencies	Fraud prevention and financial crime detection organisations	To prevent, detect, and investigate fraud, money laundering, terrorist financing, and other illicit or unlawful activity

Regulators and authorities	Regulatory bodies, supervisory authorities, law enforcement agencies, government agencies, tax authorities, courts	To comply with applicable laws, regulations, regulatory requirements, and lawful requests, or to establish, exercise, or defend legal claims
Recipients in relation to Data Subject Requests, Requests for Information, and Complaints	Competent public authorities and bodies, including law enforcement agencies, regulators, ombudsmen, arbitration bodies, courts; our corporate client to whom you made payments or with whom you interact as their end use	To comply with specific, lawful requests for information, legal or regulatory obligations (including litigation hold requirements), or court or administrative proceedings, where such disclosure is necessary, proportionate, and permitted under applicable law
Professional advisers	Auditors, legal advisers, consultants, and other professional advisers	To obtain professional advice and support for legitimate business purposes, subject to confidentiality and data protection obligations
Business transfers	Prospective or actual buyers, investors, or advisers	In connection with a merger, acquisition, restructuring
With your consent	Other third parties identified at the time consent is obtained	Where you have given your explicit consent for a specific purpose

OUR PROCESSING AND HOSTING LOCATIONS

Our website and cloud storage providers host personal data primarily within the United Kingdom (UK) and the European Economic Area (EEA). As a result, your personal data is generally stored and processed within these jurisdictions.

Transfers within the OpenPayd Group

To ensure an adequate level of protection for your personal data, we have implemented an intragroup data processing and international data transfer agreement. This agreement incorporates:

- the EU Standard Contractual Clauses adopted by the European Commission under Implementing Decision (EU) 2021/914 of 4 June 2021;
- the UK International Data Transfer Addendum, issued by the UK Information Commissioner's Office and laid before the UK Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022; and
- country specific data protection clauses.

Transfers to third-party service providers

Some of our banking partners and third-party service providers, or their sub-processors, may process or transfer personal data outside of the UK and the EEA. Where such international transfers occur, they are carried out in compliance with applicable data protection laws and are generally safeguarded by:

- the EU Standard Contractual Clauses and/or the UK International Data Transfer Addendum; or
- other recognised and lawful international data transfer mechanisms.

We take appropriate steps to ensure that all international transfers of personal data are subject to suitable safeguards and that your data remains protected.

For further information about where and how your personal data is transferred, please contact us using the details set out below.

DATA RETENTION

We will retain your personal data only for as long as is necessary to fulfil the purposes for which it was collected, including to comply with applicable legal, regulatory, tax, accounting, and reporting obligations.

In certain circumstances, we may retain personal data for a longer period, including where:

- a complaint has been raised; or
- we reasonably believe there is a prospect of litigation or a regulatory investigation.

How we determine retention periods

When determining the appropriate retention period for personal data, we take into account:

- applicable statutory and regulatory retention requirements;
- the duration of the relevant contractual relationship;
- the nature, volume, and sensitivity of the personal data;
- the potential risk of harm from unauthorised use or disclosure;
- the purposes for which the data is processed and whether those purposes can be achieved through other means; and
- applicable legal, regulatory, tax, accounting, and reporting requirements.

Retention policies and deletion

We maintain and apply a data retention policy which sets out retention periods and governs the secure deletion of personal data once it is no longer required.

As a general rule, personal data is retained until the purposes for which it is processed have been fulfilled, unless longer retention is required under applicable laws (for example, anti-money laundering, commercial, or tax legislation).

TECHNICAL AND ORGANISATIONAL MEASURES

In accordance with the applicable data protection laws, we implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of individuals. Please see our Information Security Statement to learn more.

INDIVIDUAL RIGHTS

Depending on your location, you have the following rights. These rights are subject to verification requirements and certain limitations and exceptions under applicable law.

- Right to confirmation of processing and information for processing
- Right to access
- Right of rectification/correction
- Right to data portability
- Right to restrict processing
- Right to object to processing
- Right to withdraw consent (where it is relied upon)
- Right to erasure/deletion
- Right to lodge a complaint with the relevant authority
- Right to opt-out of the sale of your personal information
- Right opt-out of the sharing of personal information
- Right to direct us not to share your personal information for cross-context behavioural advertising, even where no monetary consideration is involved
- Right to limit the use and disclosure of sensitive personal information
- Right to non-discrimination
- Right to designate an authorized agent to submit requests on your behalf, subject to verification requirements
- Right to to appeal our refusal to take action on a request
- Right to confirm the third parties or categories of third parties to which personal information has been disclosed

We work hard to ensure that we protect our customers' personal data in accordance with our legal obligations. If you are unhappy with how you think we have processed your personal data, please contact us using the details above and we will do our best to resolve your complaint.

If you do not think we have been able to resolve your complaint, you can complain to the relevant authority:

- a list of European Union data protection authorities can be found here
- the United Kingdom's data protection authority's contact details can be found here
- the California Privacy Protection Agency contact details can be found here
- The Office of the Privacy Commissioner in Canada contact details can be found here

If you have questions about what rights may apply to you or to submit a request to exercise any of the rights described above, please contact OpenPayd's Data Protection Officer (DPO).

CONTACT DETAILS

If you have any questions or concerns about this privacy notice and/or our processing of your personal data, you can contact us by using the following details:

OpenPayd Group's DPO: Mrs. Diana Karaivanova
Email: privacy@openpayd.com
UK address: SettleGo Solutions Limited, The Bower, 207-211 Old Street, London, England, EC1V 9NR
EU address: OpenPayd Financial Services Malta Limited, 122 – 123 Pangea, Level 5 , Triq San Gorg, St. Julians STJ 3204, Malta

COOKIES, TRACKING TECHNOLOGIES AND DO NOT TRACK SIGNALS

We use cookies and similar tracking technologies (such as pixels, SDKs, and web beacons) to operate our website, analyse usage, enhance functionality, and support our security and fraud-prevention efforts. Further information about the cookies we use and how to manage your preferences is set out in our Cookies Policy.

Some web browsers offer a “Do Not Track” (“DNT”) feature that allows users to signal a preference not to be tracked across websites. As there is currently no universally accepted standard for responding to DNT signals, our website does not respond to such signals.

You can control the use of cookies and similar technologies through your browser settings and, where available, through our cookie consent or preference management tools.

MISCELLANEOUS INFORMATION

No fee usually required

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

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights).

Time limit to respond

We try to respond to all legitimate requests as soon as we can, and in any event within one month of receiving your request and any necessary proof of identity or further information. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and we are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

UPDATES TO THIS PRIVACY NOTICE

We may change this privacy notice from time to time to reflect new services or changes in our privacy practices or relevant laws. The “Last updated” legend at the top of this privacy notice indicates when this notice was last materially revised. Any changes are effective on the date when we post the revised notice on our website.

GLOSSARY

Depending on the context, you might be an End User, Representative of a potential or existing corporate client of OpenPayd, Representative of our Banking Partners of Third-party Service providers, or Website Visitor:

End Users. These are our corporate clients’ customers. If you are reading this as an End User, please note that we do not have a contractual relationship with you and do not offer or provide services to you, but we receive your personal data to provide services to our corporate client, including in relation to payments you make to our corporate client.

Representative of a potential or existing corporate client. These individuals are acting on behalf of an existing or potential corporate client, such as authorised users, contact persons, directors, shareholders and controlling persons.

Representative of banking partners or third-party service providers. These individuals are acting on behalf of our partners and suppliers, such as employees, contact persons, directors, shareholders and controlling persons.

Website visitor. These individuals interact with OpenPayd by visiting our website, including using the available communication channels to obtain information regarding our services or to contact us with a query.

Personal Data refers to any information associated with an identified or identifiable individual, which can include: data provided to us directly by the individual, data that is provided to us by our corporate client, or data that is provided to us by an End User's sending bank, and or other data that we collect during provision of our services. Personal Data also includes "personal information" or its equivalent as defined in the applicable data protection laws.

Services refers to the services that we provide under our Terms to our corporate clients. We do not provide services to individuals.

Banking partners are financial institutions, banks, and other partners such as payment method acquirers, payment intermediaries, payment aggregators, infrastructure providers, payment method providers, payment processors, and networks that we partner with, directly or indirectly, to provide the Services.

Third party service providers are any other suppliers that we might use to provide the Services, including to perform sanction screening checks and transaction monitoring.

OpenPayd Group means, collectively, all companies within the OpenPayd Group. An overview of the OpenPayd Group companies is available here.