OpenPayd Data Processing Agreement

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)

Data Processing Agreement

This Data Processing Agreement (the "DPA") defines the roles and responsibilities of the Parties for their respective processing of personal data and is integral part of all business terms agreed between the Parties, including but not limited to OpenPayd terms of use, any service specific terms, additional terms, and/or country specific terms (collectively "the Terms"). The DPA shall override any other terms and any deviation thereof if and to the extent there is any conflict or inconsistency and shall survive the termination of all agreements between the Parties.

The following table sets out the different OpenPayd group entities to which this DPA applies:

Entity	**Role**
SettleGo Solutions Limited	Controller, joint controller, or processor
OpenPayd Financial Services Malta Limited	Controller, joint controller, or processor
OpenPayd Financial Services Malta Limited, French Branch	Controller, joint controller, or processor
OP Digital Services Limited	Controller or Joint Controller
OpenPayd Canada Inc.	Controller or Joint Controller

Each referred to as OpenPayd, as applicable under the relevant Terms.

1. Definitions

For the purposes of this DPA, the terms defined below shall have the following meanings.

Adequacy Decision means a European Commission Decision and/or a decision of the Secretary of State of the UK that a third country or an international organization ensures an adequate level of data protection as defined in Data Protection Law.

Adequate Country means a country that is recognized by the European Commission and/or the Secretary of State of the UK under Data Protection Law providing adequate protection for Personal Data.

Appropriate Safeguards means the standard of protection over the personal data and of data subjects' rights, which is required by Data Protection Law when parties are making a third country transfer relying on standard data protection clauses and where required, conducting a transfer risk or impact assessment in accordance with applicable guidance.

Controller means the entity which, alone or jointly with others, determines the purposes and means of Processing Personal Data, which may include, as applicable, a "Business" as defined under the CCPA.

Processor means the entity that Processes Personal Data on behalf of the Controller, which may include, as applicable, a "Service Provider" as defined under the CCPA.

Data Complaint means a complaint or request relating to either party's obligations under the Data Protection Laws relevant to the Agreement including any complaint by a data subject or any notice, investigation or other action by a Supervisory Authority.

Data Protection Law means all applicable data protection laws (and in each case any re-enactment or amendment) in any jurisdiction where we operate (to the extent applicable to the services we provide to you under the relevant Agreement), including but not limited to, the Data Protection Act 2018, the UK GDPR, the EU GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the French Data Protection Act (the "FDPA"), the Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the California Consumer Privacy Act of 2018, Cal. Civ. Code Sections 1798.100-1798.199 (the "CCPA"), any other U.S. federal, state, and local laws relating to the lawful processing of personal data, data security safeguards, confidentiality of customer information, incident and breach notification, and any other directly applicable local or national laws relating to privacy and data protection.

Data Subject Request means a request made by a data subject to exercise any rights of data subjects under the Data Protection Law in connection with the Personal Data.

EEA means the European Economic Area.

EU SCCs means the European Standard Contractual Clauses of EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021, incorporated by reference into this DPA and specified in Appendix 2.

Joint Data means the term in Section 6 – Joint Controllers terms of this DPA.

Personal Data means any information relating to an identifiable natural person that is processed in connection with the Terms defined as "personal data" under the GDPR and as "personal information" under the CCPA, including Shared Data and Processed Data as defined in this DPA.

Processed Data means the term in Section 7 – Processor terms of this DPA.

Shared Data means the term in Section 5 – Controller terms of this DPA.

Supervisory Authority means any local, national, or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board, or other body responsible for administering the Data Protection Laws including the Information Commissioner's Office in the United Kingdom, and the Information and Data Protection Commissioner in Malta.

UK means England, Scotland, Wales, and Northern Ireland.

UK Addendum means the UK International Data Transfer Addendum to the EU SCCs issued by the UK ICO and laid before UK Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, incorporated by reference into this DPA and specified in Appendix 3.

Lowercase terms if used but not defined in this DPA such as "personal data", "personal data breach", "processing", "data subject", "data subject request" have the meanings set out in the Data Protection Law.

2. Changes and Compliance with Data Protection Law

OpenPayd and Client shall comply with the provisions and obligations imposed by the Data Protection Law when processing Personal Data in connection with the Terms. Such processing shall be in respect of the types of Personal Data, categories of data subjects, nature and purposes, and duration, set out in the Appendix 1 to this DPA.

We reserve the right to update this DPA from time to time in accordance with the Terms, including in order to comply with our obligations under the Data Protection Law, to address any changes to the services including any new functionality or features and/or to cover any additional services that we may provide to you from time to time. The prevailing terms will be the terms of the most recent version of this DPA made available on the OpenPayd website and notice will be deemed to be given on the date of publication on the OpenPayd website.

3. Roles and responsibilities

In providing the services under the Terms and otherwise complying with its obligations under the Terms, OpenPayd may act as a joint controller, a controller, or a processor of Personal Data. This DPA is divided into the following sections:

General Terms – general data protection principles, applicable irrespective of the role.
Controller Terms – applicable for controller-to-controller relationship between Client and OpenPayd.
Joint Controllers Terms – applicable only where OpenPayd acts as a joint controller.
Processor Terms – applicable for controller-to-processor relationship between Client and OpenPayd.

4. General Terms

4.1. Contact details
Any queries relating to the protection of Personal Data shall be sent to OpenPayd's Data Protection Officer at privacy@openpayd.com.

4.2. Security of processing
OpenPayd and Client shall process Personal Data in accordance with the general privacy principles and in compliance with Data Protection Law and the terms of this DPA. Taking into account the state of the art, the

costs of implementation and the nature, scope, context and purposes of the processing, they shall implement appropriate technical and organisational measures and procedures to ensure a level of security for such personal data appropriate to the risk, including the risks of accidental, unlawful or unauthorised destruction, loss, alteration, disclosure, dissemination or access to the Personal Data.
OpenPayd and Client shall adopt and maintain appropriate data protection, data privacy, information security and operational resilience policies in relation to the processing of the Personal Data and procure that the staff comply, at all times, with such policies. All staff shall be subject to confidentiality obligations which cover their processing the Personal Data. Each Party is responsible for assessing whether the measures implemented by the other Party to meet its own technical and organisational measures implemented meet the requirements of the Data Protection Law.

4.3. Data Transfers
OpenPayd and Client shall not transfer any Personal Data to a country or a territory that is not deemed adequate, unless having in place Appropriate Safeguards. OpenPayd and Client shall each ensure that the Personal Data they disclose or otherwise transfer is accurate, and they have an appropriate lawful ground as set out in the Data Protection Law.
OpenPayd and Client shall not disclose or transfer to each other any excessive or irrelevant personal data that is not required in connection with the provision or receipt of the services under the Terms.

4.4. Audits
Parties shall be able to demonstrate compliance and document and maintain accurate, complete, and up to date records of their processing activities in accordance with the requirements of the Data Protection Law. Any audits and inspections shall be kept strictly confidential unless required otherwise by the relevant regulatory authority, in which case, to the extent legally permissible, OpenPayd and Client shall give each other a prior notice.

4.5. Purposes of processing of Personal Data
OpenPayd and Client shall process the Personal Data only for the purposes of provision or receipt of the services under the Terms, including for compliance with their legal and regulatory obligations.
Personal Data shall be retained for no longer than is necessary for the above-mentioned purposes.

4.6. Lawful processing
The Client represents and warrants that it has taken, and shall continue to take, all measures necessary to ensure that OpenPayd may lawfully Process Personal Data in accordance with all applicable Data Protection Laws.

Without limitation, the Client represents, warrants and undertakes that:

4.6.1. Lawful Basis
The Client has identified and maintains at all times a valid and appropriate lawful basis for the Processing of Personal Data, including, where applicable, the disclosure or transfer of such Personal Data to OpenPayd, whether directly by the Client or indirectly via third-party infrastructure or service providers.

4.6.2. End-User Transparency and Notices
The Client has provided, and shall ensure that it continues to provide, clear, accurate and complete privacy notices to all relevant data subjects (including its end users), which expressly identify OpenPayd as a regulated payment services provider involved in the provision of payment accounts, including named virtual IBANs allocated to their end-users names and related payment services; clearly describe OpenPayd's role in the Processing of Personal Data (including whether OpenPayd acts as a processor, controller, or independent controller, as applicable under the relevant services); comply in all respects with the transparency requirements set out in the GDPR (or equivalent provisions under applicable Data Protection Law).

4.6.3. Authority to Share Personal Data
The Client has obtained all necessary authorisations, consents (where required), and confirmations from data subjects to enable the lawful disclosure of their Personal Data to OpenPayd for the purposes contemplated under the Terms and the DPA.

4.6.4 Accuracy and Ongoing Compliance

The Client shall ensure that all information provided to data subjects regarding the use of OpenPayd and the Processing of Personal Data remains accurate, up to date, and consistent with the services provided and the applicable Terms.

4.7. Data Subject Requests and Data Complaint Handling

Each party shall handle any Data Subject Request, Data Complaint, or regulatory or supervisory complaint (including any inquiry, investigation, or request for information from a data protection authority, financial regulator, ombudsman, or other competent authority) relating to its Processing of Personal Data in a timely, transparent, and professional manner and in accordance with applicable Data Protection Law and regulatory requirements.

Where OpenPayd receives a Data Subject Request, Data Complaint, or regulatory or supervisory inquiry that relates, in whole or in part, to the Client's Processing of Personal Data, or where it is otherwise necessary in order to respond lawfully and appropriately to such request, complaint, or inquiry, OpenPayd may: share the Client's relevant contact details with the data subject, regulator, supervisory authority, or ombudsman; refer the data subject or authority to the Client for further handling of the matter; and disclose such information as is strictly necessary to comply with its legal and regulatory obligations.

Each party shall provide reasonable and timely cooperation to the other in connection with any Data Subject Request, Data Complaint, or regulatory or supervisory inquiry, including by providing relevant information and assistance where required, without prejudice to each party's status as an independent data controller and without assuming responsibility for the other party's compliance failures.
Nothing in this clause shall require either party to disclose information subject to legal privilege or that would otherwise be unlawful to disclose.

5. Controller Terms

Where OpenPayd processes Personal Data as an independent controller under or otherwise in connection with the Terms ("Shared Data"), the provisions set out in this Part 5 Controller Terms will apply to the processing of Shared Data by OpenPayd, in addition to Section 4 – General Terms.
OpenPayd will comply with its controller obligations under the Data Protection Law in connection with its processing of Shared Data to provide the services to the Client and to comply with a legal obligation.
OpenPayd shall process the Shared Data solely for purposes for which the data has been obtained.

If Client or OpenPayd receive or become aware of any of the following, it shall notify without any undue delay the other Party of the following and provide a reasonable assistance to each other to comply with their reporting obligations under the Data Protection Law:

(i) any breach of security or unauthorised access to Disclosed Personal Data without undue delay after becoming aware of such incident; and
(ii) any complaint, inquiry or request from a data subject or data protection authority regarding Shared Data, unless such notice is prohibited by applicable law.

Client and OpenPayd shall refrain from notifying or responding to any data subject or data protection authority on behalf of the other Party unless:

(i) specifically requested to do so by the other Party in writing; or
(ii) if required by the Data Protection Law.

Client acknowledges and agrees that OpenPayd, at its sole discretion, may disclose any Shared Data or other transaction-related information to the relevant regulatory authorities or to third parties in order to perform their obligations under the Terms and/or legal/regulatory obligations under the relevant law, including but not limited to anti-money laundering, fraud monitoring, sanctions, or as may otherwise be required by the relevant law or court order.

Each Party shall respond to Data Subject Requests relating to its own processing of Shared Data.

5.1. Data Subject Requests and Data Complaint
If a party receives a Data Subject Request and/or a Data Complaint relating to the processing of Joint Data, it will promptly notify the other party, and in any event within three business days of receipt of the Data Subject Request and comply with the provisions of this paragraph. As between the parties, responsibility for compliance with and responding to (i) any Data Subject Request falls on the party which first received such Data Subject Request; and (ii) any Data Complaint regarding the processing of Joint Data falls on the party which receives the Data Complaint, unless agreed otherwise by the parties. The parties will provide reasonable assistance to one another to assist with handling Data Subject Requests and Data Complaints relating to the processing of Joint Data. Each party will deal with a Data Subject Request or a Data Complaint relating to the processing of Joint Data, in a timely and professional manner and in accordance with the requirements of the Data Protection Law.

Neither party will respond to a Data Subject Request or Data Complaint relating to the processing of Joint Data, without consultation with the other party, unless such failure to respond would cause it to be in breach of the Data Protection Laws and/or it is requested to respond by a Supervisory Authority.

5.2. Personal Data Breaches
If a Personal Data Breach occurs in relation to the Joint Data processed by either party, the party that discovers the Personal Data Breach will notify the other party without undue delay (and in any event within 48 (forty-eight) hours of becoming aware of the Personal Data Breach), and will provide a detailed description of the Personal Data Breach, including the details of the type of data and the identity of the affected person(s) as soon as such information can be collected or otherwise becomes available, as well as any other information that the other party may reasonably request from time to time;
The parties will reasonably cooperate to determine the cause of the Personal Data Breach and who should notify the Supervisory Authority and/or the data subject(s) if required.

6. Joint Controllers Terms

Where OpenPayd process Personal Data as a joint controller under or otherwise in connection with the Terms ("Joint Data"), the provisions set out in this Section 6 will apply for the processing of Joint Data, in addition to Section 4 and 5. In case of any conflict between the provisions in Section 4, 5 and in Section 6, Section 6 will prevail.

The parties will comply with their controller obligations under the Data Protection Law in connection with its processing of Joint Data.

The parties agrees that:
(i) for the Joint Data, the joint controllers act together to determine the purpose and means of processing;

(ii) the joint controllers will process the Joint Data solely for the provision of the Services under the Terms and in accordance with Appendix 1 as updated from time to time;
(iii) the joint controllers will ensure that any data subject who wants to make a Data Subject Request has an easily accessible point of contact to do so;
(iii) the joint controllers will ensure that the Joint Data has been collected, processed, and transferred in accordance with the Data Protection Law as applicable to that Joint Data;

The parties will be responsible for providing all necessary, fair and transparent information and notices to data subjects.

The parties will provide reasonable assistance to each other to assist with handling Data Subject Requests, breach notification requirements, data protection impact assessments and any other reasonable support necessary for the party to comply with its its controller obligations under the Data Protection Law in connection with its processing of Joint Data.

6.1. Conditional Joint Controllership for New Services
Where, in connection with the Terms, the Client requests or agrees to the provision of a new or additional service by an OpenPayd entity that requires coordinated Processing of Personal Data by the Client and such OpenPayd entity, the Client acknowledges that OpenPayd and the relevant OpenPayd entity may act as joint controllers (or the equivalent concept under applicable Data Protection Law) solely in respect of the Processing of Personal Data that is strictly necessary to onboard the Client and to efficiently provide and enable such new or additional service.

For these limited purposes, the Client expressly authorises OpenPayd to share relevant Personal Data with the other joint controller, including by means of automated data exchange through application programming interfaces (APIs), where such sharing is necessary to: (i) complete onboarding, due diligence, and verification activities; (ii) facilitate the expedited provisioning, configuration, and activation of the requested services; and (iii) ensure regulatory and operational compliance in connection with such services.

The parties shall determine, in good faith and prior to or in parallel with the commencement of such Processing, their respective responsibilities for compliance with applicable Data Protection Law in accordance with Article 26 of the GDPR (or equivalent provisions), including transparency obligations and the handling of Data Subject Requests, and shall make the essence of such arrangement available to data subjects as required by law.

OpenPayd shall remain responsible for ensuring that any such data sharing is carried out in a secure, lawful, and transparent manner.

7. Processor Terms

Where OpenPayd acts as a Processor or as a Service Provider, or equivalent role under Data Protection Law in relation to the Processed Data under, or otherwise in connection with, the Terms, the provisions set out in this Section 7 shall apply in addition to Section 4 (General Terms). In the event of any conflict between Section 4 and Section 7, the provisions of Section 7 shall prevail.

7.1. Data Accuracy and Data Minimisation
The Client shall ensure that any Personal Data provided to OpenPayd, incdluding end user Personal Data under the Terms via API or through other means is accurate, complete, and kept up to date for the purposes of the Data Processing for the duration of the Agreement.

The Client shall ensure that the Personal Data provided to OpenPayd is lawful, adequate, relevant, and limited to what is strictly necessary in relation to the specified and documented purposes of the Data Processing.

OpenPayd shall be entitled to rely on the Client's compliance with the obligations set out in this clause and shall not be responsible for verifying the accuracy or completeness of the Personal Data provided by the Client except to the extent required by applicable law.

7.2. Documented instructions

OpenPayd shall, unless required to do otherwise by applicable law, process the Processed Data only on and in accordance with the Terms and any other documented instructions from Client.
If any applicable law requires OpenPayd to process Processed Data other than in accordance with the Client document instructions, OpenPayd shall notify Client of any such requirement before processing the Processed Data (unless any applicable Laws prohibit such information on important grounds of public interest).

To the extent the CCPA applies and OpenPayd is acting as a Data Processor, OpenPayd will not (except to provide OpenPayd's services as permitted by applicable law): (i) sell or share (as defined under the CCPA) Processed Data; (ii) retain, use or disclose Peocessed Data outside of its direct business relationship with Client other than to provide services under the Terms and as required to comply with applicable law; and (iii) combine any Processed Data it receives on Client's behalf with any personal data received from other controllers or received from any interactions with Client's end users, unless specifically permitted under the CCPA; OpenPayd shall comply with the requirements in this DPA relating to the CCPA and will provide the same level of privacy protection to Processed Data as required by the CCPA. For avoidance of doubt, Personal Data transmitted to OpenPayd in the course of executing transactions on behalf of the Client shall be deemed Personal Data received on behalf of the Client, and not from the Service Provider's own interaction with the end user (consumer).
OpenPayd will inform Client if it determines that it can no longer meet its obligations under the Data Protection Law and will take reasonable and appropriate steps to remediate any unauthorized processing of Personal Data.

7.3. Confidentiality and Security

OpenPayd shall implement and maintain appropriate technical and organisational measures as defined in our Information Security Statement, and incorporated by reference to this DPA, to ensure a level of security of Processed Data appropriate to the risk required pursuant to Data Protection law and adequate protection of the Processed Data, having regard to the state of technological development and the cost of implementing any measures. Any subsequent versions of the Information Security Statement shall be applicable to this DPA and its content will be no less stringent than its previous version. OpenPayd shall keep Processed Data confidential and will ensure its staff and Subprocessors are bound by the same confidentiality obligation.

7.4. Audits and Cooperation

OpenPayd shall reasonably co-operate and assist the Client to comply with its obligations under the Data Protection Law, such as forwarding any data subject requests or verifiable consumer requests as defined under the CCPA, or their equivalent, relating to Processed Data to Client without undue delay, providing information for the processing of Processed Data in relation to data protection impact assessments, inspections, and notifications to data protection authorities. On reasonable request and notice, OpenPayd will co-operate in the conduct of any audit or inspection, reasonably necessary to demonstrate OpenPayd's compliance with its obligations as a processor under this DPA. Client shall avoid causing any damage, injury, or disruption to OpenPayd's equipment, staff and business in the course of such audit or inspection.

7.5. Breach Notification

In the event of a personal data breach concerning Personal Data processed by OpenPayd, OpenPayd shall notify the Client without undue delay, after OpenPayd having become aware of the breach. Such notification shall contain, at least:
(i) description of the nature of the personal data breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);
(ii) likely consequences of the personal data breach;
(ii) measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects;
(iv) the details of a contact point where more information concerning the personal data breach can be obtained.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. OpenPayd shall fully assist the Client in assessing and notifying the personal data breach to the competent supervisory authority, and in complying with the obligation to communicate the personal data breach to the data subjects, where relevant.

7.6. Sub-processors

Client generally agrees that OpenPayd may engage third party providers with regards to the Processed Data ("Sub-processors"). OpenPayd shall make available to Client the current list of Sub-processors, attached as an Appendix 1 to this DPA.If OpenPayd engages a new Sub-processor, OpenPayd must inform Client of the intended engagement and Client may object to the intended engagement of such new Sub-processor by notifying OpenPayd within 10 (ten) business days of the notification, provided that such objection must be on reasonable, substantial grounds, directly related to such new Sub-processor's ability to comply with substantially similar obligations to those set out in this DPA. If Client does not object, the engagement of the new Sub-processor shall be deemed accepted by Client. OpenPayd shall ensure that the contract with each new Sub-processor shall impose obligations on the new Sub-processor that are substantially equivalent to the terms of this DPA.

With respect to each Sub-processor, OpenPayd shall enter into a written contract with the Sub-processor to ensure that at least the same level of protection will be given to Personal Data as that required by the Terms and this DPA and, in substance, the same data protection obligations as those binding OpenPayd under this DPA.

7.7. Data Transfers

OpenPayd may process Processed Data globally as necessary to perform the services under the Terms. To the extent such global access involves a third country transfer of Processed Data subject to cross-border transfer obligations under Data Protection Law within the OpenPayd group, OpenPayd's Intragroup Data Transfer Agreement will apply.

If and to the extent the processing of Processed Data involves a transfer of Processed Data to Sub-processor or other business partners located outside of the UK and the EEA, OpenPayd shall conduct a transfer risk or impact assessment where required. The Parties agree that Processed Data may only be transferred, if:

(i) the transfer is to a jurisdiction for which an appropriate EU and/ or UK Adequacy Decision has been issued and subject to the terms of that Adequacy Decision;
(ii) in the absence of an Adequacy Decision, the transfer is subject to Appropriate Safeguards.

7.7. Return and deletion of data

On termination of the Terms, and Client's written request, OpenPayd will return any Processed Data to the Client or securely destroy it to the extent legally permissible (i.e. storage of Processed Data is required by the relevant laws, in which case OpenPayd will be entitled to retain the same in accordance with the relevant laws). For the avoidance of doubt, OpenPayd may retain Personal Data for the duration of any statutory anti-money laundering, financial crime, or other regulatory retention periods that apply to its business.

Appendix 1 - Details of processing

Categories of data subjects whose Personal Data is processed by OpenPayd

Client-Related Data Subjects (any identified or identifiable natural persons) whose Personal Data is processed by OpenPayd on behalf of the Client in connection with the services under the Terms, including, as applicable:

- the Client's end users for the purposes of issuing named virtual IBANs.
- directors, officers, and authorised signatories;
- shareholders and ultimate beneficial owners;
- employees and other authorised users; and
- any other individuals whose Personal Data is provided to OpenPayd by or on behalf of the Client, or otherwise processed at the Client's instruction in connection with the services.

Categories of personal data processed by OpenPayd

- Named virtual IBAN (vIBAN) data relating to end users;
- Identity and verification data, including KYC/KYB information;
- Contact information;
- Sanctions screening and transaction monitoring data;

- Payments and account data;
- Foreign exchange (FX) and digital asset trading-related data; and
- Any other Personal Data processed at the Client's instruction in connection with the Services.

Sensitive Data
If applicable, OpenPayd may process special categories of personal data or sensitive data (e.g., biometric data).

Nature and purpose for which the personal data is processed on behalf of the Client
For the purposes of allocation of named virtual IBANs of Client's end users- name, date of birth, address/country.

Processing of Personal Data such as collection, use, storage, combination, erasure, transmission, disclosure, or otherwise making available, and any other operation necessary for provision of the services under the Terms.

Frequency and Duration of the processing
On continuous basis for the duration of the Terms
For the duration of the Terms and for such time as required by the applicable law

For processing by (sub-)processors, also specify subject matter, nature and duration of the processing
Same as above
Technical and organizational measures, including measures to ensure the security of data
As specified in the Information Security Statement

List of Sub-processors:
OpenPayd group entities
Customer management services – Salesforce, Microsoft, Slack
Cloud services –Google Cloud Platform (data storage in Belgium)

Appendix 2 – EU SCCs specification

To the extent legally required, by signing this DPA, Client and OpenPayd are deemed to have signed the EU SCCs as an additional safeguard, which form part of this DPA and will be deemed completed as follows:

Module 1 of the EU SCCs applies to transfers of Personal Data from Client (as a Controller) to OpenPayd (as a Controller) and Module 2 applies to transfers of Personal Data from Client (as a Controller) to OpenPayd (as a Processor).

Clause 7 of the EU SCCs (the optional docking clause) is included.

For Module 2, under Clause 9 of the EU SCCs, the Parties select Option 2 (General written authorization). OpenPayd shall specifically inform the Client in writing of any intended changes to the list through the addition or replacement of sub-processors at least 10 (ten) business days in advance, thereby giving the Client sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s).

Under Clause 11 of the EU SCCs, the optional language requiring that Data Subjects are permitted to lodge a complaint with an independent dispute resolution body shall be deemed to be included.

Under Clause 17 of the EU SCCs, the Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights). The Parties select the laws of Ireland.

Under Clause 18 of the EU SCCs (Choice of forum and jurisdiction), the Parties select the courts of Ireland.

Annex I(A) and I(B) is completed as set forth in Appendix 1.

Under Annex I(C), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission.

Annex II is completed as provided in the Information Security Statement.

Annex III is completed as provided in Appendix 1 of this DPA for clarity.

Appendix 3 – UK Addendum

With respect to Personal Data transferred from the UK, the UK Addendum to the EU SCCs forms part of this DPA and takes precedence over the rest of this DPA as set forth in the UK Addendum.

The UK Addendum shall be deemed complete as follows:

In table 1 of the UK Addendum, the Parties' details shall be the Parties and their Affiliates to the extent any of them are involved in such transfer and are specified in the Terms.

In table 1 of the UK Addendum, the Key Contacts shall be the contacts set forth in the Terms.
In table 2 of the UK addendum, the Approved EU SCCs referenced in Table 2 of the UK Addendum shall be the EU SCCs as executed by the Parties; Personal data received from the exporter can be combined with personal data collected by the importer.

In table 3 of the UK Addendum, Annex I(A) and I(B) is completed as set forth in Appendix 1.

In table 3 of the UK Addendum, Annex II is completed as provided in the Information Security Statement.

In table 3 of the UK Addendum, Annex III is completed as provided in Appendix 1 of this DPA for clarity.

In table 4 of the UK Addendum, either Party may end this DPA as set out in Section 19 of the UK Addendum.

By entering into this DPA, the Parties are deemed to be signing the UK Addendum.

To the extent there is any conflict or inconsistency between the EU SCCs or UK Addendum and any other terms in this DPA or the Terms, the provisions of the EU Standard Contractual Clauses or UK Addendum, as applicable, will prevail.

Appendix 4 – Swiss Addendum to the EU SCCs

Where a transfer of personal data from a Data Exporter to a Data Importer is subject to both the Regulation (EU) 2016/679 (EU GDPR) and the Swiss Federal Act on Data Protection (as defined below), the following provisions shall apply in order for the EU Standard Contractual Clauses (the "SCCs") to ensure an adequate level of data protection in accordance with Article 6 paragraph 2 letter a of the FADP and, where applicable, the Revised FADP.

In the event of any conflict between this Swiss Addendum and the SCCs, this Swiss Addendum shall prevail solely with respect to data transfers governed by Swiss data protection law.

1. **Definitions**

For the purposes of this Swiss Addendum:

"FADP" means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1), as amended from time to time.

"Revised FADP" means the revised Swiss Federal Act on Data Protection of 25 September 2020, as in force from 1 September 2023.

"FDPIC" means the Swiss Federal Data Protection and Information Commissioner.

2. Application to Swiss Data Subjects

Any reference in the SCCs to "data subjects" shall be understood to include data subjects in Switzerland. Any reference to the "EU GDPR" shall be construed as a reference to the FADP or the Revised FADP, as applicable, insofar as the relevant data transfer is governed by Swiss data protection law.

3. Competent Supervisory Authority

Where the data transfer is governed by the FADP or the Revised FADP, the FDPIC shall act as the competent supervisory authority within the meaning of the SCCs.

4. Jurisdiction and Venue

Any reference in the SCCs to an "EU Member State" shall not be interpreted in a manner that excludes data subjects in Switzerland from exercising their rights before the competent courts of their place of habitual residence in Switzerland, in accordance with Clause 18(c) of the SCCs.

5. References to Union Law

Any reference in the SCCs to "Union law" or "EU law" shall be interpreted, where necessary, as a reference to Swiss law, including the FADP or the Revised FADP, for data transfers subject to Swiss data protection law.