DEUSXPAY

DATA PROTECTION ADDENDUM

Last Update: August 2026

DEUSXPAY

SECTION A

STRUCTURE OF THIS ADDENDUM

1.1 This Addendum is comprised of the following sections and documentation:

1.1.1 **Section A (Structure of this Addendum)**, which provides an overview of the structure of this Addendum;

1.1.2 **Section B (Glossary and Defined Terms)**, which sets out the definitions used in this Addendum and how key terms are interpreted;

1.1.3 **Section C (Technical and Organisational Measures)**, which sets out the general terms and conditions applicable to all processing of Personal Data under this Addendum;

1.1.4 **Section D (Joint Controller Terms)**, which sets out the terms that apply where we and you act as joint controllers of Personal Data;

1.1.5 **Section E (Controller Terms)**, which sets out the terms that apply where we act as an Independent Controller of Personal Data;

1.1.6 **Section F (Processor Terms)**, which sets out the terms that apply where we act as a processor of Personal Data on your behalf;

1.1.7 **Schedule 1 (Details of Personal Data)**, which describes the categories of Personal Data, Data Subjects, and the purposes of processing;

1.1.8 **Schedule 2 (Cross-Border Transfer Mechanisms)**, which sets out the mechanisms governing international transfers of Personal Data;

1.1.9 **Schedule 3 (Sub-Processors)**, which sets out the list of sub-processors used by Deus X Pay, as at the date of the last revision of this Addendum; and

1.1.10 Any other policies, procedures, annexures, or documents referenced in this Addendum or incorporated by reference (together, the "Addendum Documents"),

(collectively, the "Addendum").

1.2 This Addendum forms part of, and is incorporated into, the Agreement.

DEUSXPAY

SECTION B

GLOSSARY AND DEFINED TERMS

This Data Protection Addendum (the "Addendum") is incorporated into and forms part of the Master Services Agreement (the "Agreement") you have entered into with Deus X Pay International Ltd, a company incorporated and registered under the laws of Canada, bearing registration number 2026416814, registered as a Money Services Business (MSB) with FINTRAC (registration number C100000383) and registered as a Payment Service Provider (PSP) with the Bank of Canada (BOC), and trading under the name "Deus X Pay", as well as all of its affiliates, holding companies, and subsidiaries ("DXP", "we", "us" or "our").

Within the scope of the provision of the DXP Services under the Agreement, it is necessary for the processor to deal with Personal Data for which a Data Subject acts as the data controller within the meaning of the Data Protection Laws. This Data Processing Addendum specifies the rights and obligations of the Parties under the Data Protection Laws in connection with the processor's handling of Personal Data.

In the event of any conflict between this Addendum and the provisions of the Agreement or our Privacy Policy, this Addendum shall prevail in relation to the protection and processing of Personal Data.

1. GLOSSARY OF DEFINED TERMS AND INTERPRETATION

1.1 Unless the context indicates otherwise, capitalised terms used in this Addendum shall have the meaning given to them below, or as otherwise defined in the Agreement:

1.1.1 "**Applicable Laws**" means any laws, regulations, regulatory constraints, obligations or rules in Canada or any relevant jurisdiction that applies to the Agreement and this Addendum (including binding codes of conduct and binding statements of principle incorporated into such rules, together with the federal Personal Information Protection and Electronic Documents Act ("PIPEDA"), the Proceeds of Crime (Money Laundering) and Terrorist Financing Act administered by the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC"), the Retail Payment Activities Act ("RPAA") administered by the Bank of Canada, and any applicable Canadian provincial private-sector privacy legislation (including Quebec's Law 25, Alberta's PIPA and British Columbia's PIPA)), interpreted where relevant in accordance with any guidance, code of conduct, or similar document published by a relevant regulatory authority.

1.1.2 "**Appropriate Safeguards**" means such legally enforceable mechanisms for transfers of Personal Data as may be permitted under the Data Protection Laws.

1.1.3 "**Commencement Date**" means the effective date of the Agreement.

1.1.4 "**Controller Data**" means any Personal Data processed by us in our capacity as an Independent Controller, as described in Section E (Controller Terms) of this Addendum.

1.1.5 "**Data Complaint**" means any complaint or request relating to either party's obligations under the Data Protection Laws in connection with the Agreement, including any complaint by a Data Subject or any notice, investigation or other action by a Supervisory Authority.

1.1.6 "**Data Processing Term**" means the duration of the Agreement and such additional period as may be required by the Applicable Laws.

1.1.7 "**Data Protection Laws**" means all applicable data protection laws (and any re-enactment or amendment thereof) in any jurisdiction where we operate, to the extent applicable to the DXP Services we provide to you, including the the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"), any applicable Canadian provincial private-sector privacy legislation (including Quebec's Law 25, Alberta's PIPA and British Columbia's PIPA), and any other directly applicable local or national regulations or directives relating to privacy.

1.1.8 "**Data Subject**" means an identified or identifiable natural person whose Personal Data is processed by us, including, without limitation:

1.1.8.1 employees, consultants, contractors, directors, shareholders, beneficial owners, authorised users, partners or trustees, including natural persons identified in any corporate due diligence, KYB or onboarding documentation provided by or in respect of our business clients;

1.1.8.2 suppliers, customers and end users; and

1.1.8.3 job applicants;

1.1.9 "**Data Subject Request**" means a request made by a Data Subject to exercise any of their rights under the Data Protection Laws regarding Personal Data.

1.1.10 "**DXP Services**" means conversion services and all related services that Deus X Pay may provide to you from time to time under the Agreement and the Service Schedules (Service Schedule 1 – 6), including but not limited to the following:

1.1.10.1 access to the DXP Platform; and

1.1.10.2 any other ancillary services that may be provided from time to time.

1.1.11 "**Independent Controller**" means a Party acting independently to determine the purposes and means of processing Personal Data, as further described in Section E (Controller Terms) of this Addendum.

1.1.12 "**Joint Data**" means any Personal Data processed jointly by the Parties as Joint Controllers under this Addendum.

1.1.13 "**Permitted Purpose**" has the meaning ascribed to it in clause 1.5 of Section C (Technical and Organisational Measures) of this Addendum.

1.1.14 "**Personal Data**" means any information relating to a Data Subject that is collected and processed by us in our capacity as a Joint Controller, Independent Controller or processor in connection with the Agreement. The types of Personal Data we process are set out in Schedule 1 to this Addendum.

1.1.15 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by us.

1.1.16 **"Security Measures**" means the data security measures described in clause 2 of Section C (Technical and Organisational Measures) of this Addendum.

1.1.17 "**Supervising Authority**" means any local, national, or multinational agency, department, official, parliament, public or statutory person, or any governmental, professional, regulatory, or supervisory body responsible for administering the Data Protection Laws, including without limitation the Office of the Privacy Commissioner of Canada ("OPC"), FINTRAC and any applicable Canadian provincial privacy commissioners.

1.2 Terms used but not defined in this Addendum, including "processing", "processor", "sub-processor", "controller", "joint controller", "data importer", and "data exporter", shall have the meanings given to them in the Data Protection Laws. Where a Data Protection Law does not formally define a term used in this Addendum (in particular PIPEDA, which uses "organization" and "third party"), the closest equivalent concept under that law shall apply, and references to a "controller" and "processor" shall be read accordingly.

1.3 This Addendum is further divided into the following Sections:

1.3.1 Section C: Technical and Organisational Measures – these terms apply irrespective of whether we act as controller, joint controller, or processor;

1.3.2 Section D: Joint Controller Terms – these terms apply where the Parties act as joint controllers;

1.3.3 Section E: Controller Terms – these terms apply where we act as an Independent Controller; and

1.3.4 Section F: Processor Terms – these terms apply where we act as a processor.

1.4 If there is any conflict between the provisions of Section C (Technical and Organisational Measures) and Sections D (Joint Controller Terms), E (Controller Terms), or F (Processor Terms), the provisions of Sections D, E, or F, respectively, will prevail to the extent of the conflict.

1.5 We reserve the right to revise, update, or amend this Addendum from time to time in accordance with the terms of the Agreement in order to:

1.5.1 comply with our obligations under the Data Protection Laws;

1.5.2 reflect any changes in our practices, legal obligations or the functionality or features of the DXP Services; and

1.5.3 cover the addition of any new DXP Services that we may provide to you from time to time.

1.6 The prevailing terms will be those of the most recent version of this Addendum made available on our Website.

1.7 Where required by law or where the changes are material, we will notify you in advance by appropriate means, such as email. Otherwise, notice will be deemed given on the date the revised Addendum is published on our Website.

DEUSXPAY

SECTION C

TECHNICAL AND ORGANISATIONAL MEASURES

1. SCOPE, PURPOSE AND APPLICATION

1.1 This Addendum sets out the procedures we shall adhere to and the additional terms, requirements, and conditions under which we will process Personal Data.

1.2 When providing the DXP Services to you and exercising or performing our rights and obligations under the Agreement, we may act as an Independent Controller, joint controller or processor of Personal Data provided to us by you.

1.3 This Addendum is intended to ensure that all processing is conducted in accordance with Applicable Laws and Data Protection Laws, and with full respect for the rights of Data Subjects.

1.4 The terms and conditions outlined in this Addendum do not reduce or replace either Party's obligations under the Data Protection Laws in relation to the protection of Personal Data.

1.5 This Addendum applies to all processing of Personal Data carried out during your onboarding as our client and throughout the course of our ongoing client relationship. We will only process Personal Data for the following reasons (collectively, the Permitted Purpose):

1.5.1 the provision of our DXP Services to you;

1.5.2 in contemplation of the provision of our DXP Services to you;

1.5.3 the performance and exercise of our rights and obligations under the Agreement;

1.5.4 compliance with our legal and regulatory obligations, including but not limited to, anti-money laundering ("AML"), counter-terrorism financing ("CTF"), tax obligations, and know-your-customer ("KYC") regulations, in accordance with FINTRAC obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and applicable Canadian privacy and AML guidance;

1.5.5 our legitimate business purposes, provided such purposes do not override your fundamental rights and freedoms as a Data Subject, and are in compliance with the reasonable purposes test under section 5(3) of PIPEDA together with any applicable consent or exception provisions under sections 7(1) to 7(3) of PIPEDA;

1.5.6 the monitoring and prevention of suspicious activities and fraud; and

1.5.7 any other reason outlined in our Privacy Policy or permitted under PIPEDA and applicable Canadian provincial privacy legislation.

1.6 We shall not process Personal Data in a way that is incompatible with these Permitted Purposes. Where any provision of this Addendum references a standard or level of protection drawn from PIPEDA, the same standard shall apply as the **minimum** standard of protection for all Personal Data processed under this Addendum. This shall not, however, displace or reduce any more specific or stricter requirement imposed by any applicable Canadian provincial Data Protection Law (including Quebec's Law 25, Alberta's PIPA and British Columbia's PIPA).

1.7 We will maintain any valid registrations, approvals, and licenses as required by Applicable Law, including registrations with FINTRAC and notification obligations to the Office of the Privacy Commissioner of Canada ("OPC") and any applicable provincial privacy commissioners, and shall pay any fees that are necessary to lawfully conduct the data processing activities covered by this Addendum.

1.8 Data processing shall take place in Canada, with remote employees in the United Kingdom (UK) and South Africa (including but not limited to).

1.9 Any relocation to a third country by the processor shall only be permitted with the express and documented consent of the Data Subject. Insofar as sub-processors are to be commissioned in third countries, the regulations in Section F (Processor Terms) shall apply.

1.10 This Addendum shall subsist for the Data Processing Term. The relevant notice period for termination shall be identical to that of the Agreement, insofar as no further obligations or rights of termination arise from the following provisions.

1.11 Termination of this Addendum, without the need for any further declaration or action, shall result in a termination of the Agreement. Likewise, termination of the Agreement, without the need for any further declaration or action, shall result in a termination of this Addendum. An isolated termination of this Addendum is not possible.

1.12 Any queries relating to this Addendum or our processing of Personal Data should be sent to security@deusxpay.com, which will be directed to our Privacy Officer. This is a role-based mailbox maintained for operational resilience and continuity, and is monitored by our Privacy Officer (who also serves as our Chief Information Security Officer accountable for compliance with PIPEDA).

2. DATA SECURITY MEASURES

2.1 We shall implement and maintain appropriate technical and organisational security measures in accordance with the Safeguards Principle (Principle 4.7) under PIPEDA and any applicable Canadian provincial privacy legislation, to ensure:

2.1.1 the level of security is proportionate to the nature, scope, and sensitivity of the Personal Data, and proportionate to the risks associated with its processing;

2.1.2 our systems for processing Personal Data comply with the Data Protection Laws and protect the rights of Data Subjects; and

2.1.3 the confidentiality, integrity, availability and resilience of our processing systems, and protection against unauthorised or unlawful processing, accidental loss, destruction, or damage of Personal Data.

2.2 Our technical and organisational security measures (the "Security Measures") include:

2.2.1 limiting access to Personal Data to authorised personnel or those with a legitimate need to know, using user and logical segmentation and controls such as conditional access and multi-factor authentication;

2.2.2 pseudonymising and/or encrypting Personal Data stored or transmitted over public or wireless networks; and

2.2.3 using firewalls and intrusion detection and prevention systems to segregate environments and detect unauthorised access; and

2.2.4 implementing and maintaining business continuity, disaster recovery, and related policies to ensure the confidentiality, integrity, availability, and resilience of processing systems, and timely access to Personal Data in the event of a physical or technical incident.

2.3 The Security Measures shall be regularly tested, assessed, and evaluated to confirm their effectiveness. We shall maintain records of such testing and review the measures periodically, updating them as necessary throughout the Data Processing Term.

2.4 We shall ensure that all personnel involved in processing Personal Data receive appropriate training on the Security Measures and applicable Data Protection Laws. The level, content, and frequency of training will be proportionate to each individual's role and responsibilities.

2.5 All personnel are subject to written confidentiality obligations covering their processing of Personal Data.

3. CROSS-BORDER DATA TRANSFERS

3.1 **Transfers Between the Parties**

Where your use of the DXP Services requires us, under the Data Protection Laws, to implement an onward transfer mechanism to lawfully and securely transfer Personal Data from Canada to your jurisdiction (if you are located outside of Canada and we are required to have Appropriate Safeguards in place) ("Transfer Mechanism"), the terms set out in Schedule 2 of this Addendum will apply.

3.2 **Transfers to Third Parties**

3.2.1 We will not transfer, access or process Personal Data outside of Canada, including through a sub-processor located in such country or territory, unless one of the following conditions are met:

3.2.1.1 the transfer satisfies the accountability principle under PIPEDA and any applicable Canadian provincial privacy legislation, and the destination country or territory provides a comparable level of protection; or

3.2.1.2 we have ensured that such transfer complies with the Data Protection Laws by having in place Appropriate Safeguards, and we have taken steps to satisfy ourselves that the level of protection afforded to the Personal Data in the destination country or territory is comparable to the level of protection it would be afforded in Canada. These Appropriate Safeguards may include:

3.2.1.2.1 a legally binding and enforceable instrument between public authorities or bodies;

3.2.1.2.2 standard contractual clauses and binding corporate rules consistent with PIPEDA and applicable Canadian provincial privacy legislation; and

3.2.1.2.3 a code of conduct or certification mechanism, along with enforceable commitments by the data importer to, *inter alia*, provide us with relevant information relating to the destination country or territory and the laws applicable to the transfer in that destination country, and of any development affecting or likely to affect the level of protection your transferred Personal Data receives in the importer's country.

3.3 If, for whatever reason, the transfer of Personal Data pursuant to paragraphs 3.2.1.1 and 3.2.1.2 ceases to be lawful, we will immediately implement other Appropriate Safeguards and ensure that the level of protection afforded to the Personal Data in the destination country or territory is comparable to the level of protection that it would be afforded in Canada.

3.4 Where we are unable to implement such safeguards, we will cease the transfer of Personal Data, unless you expressly authorise the transfer to continue.

4. ENGAGMENT OF PROCESSORS AND SUB-PROCESSORS

4.1 If we identify a need to engage a processor or sub-processor to perform any processing activities in respect of Personal Data, we will:

4.1.1 enter into a written contract with each processor or sub-processor which imposes the same data protection obligations as set out in this Addendum and our Privacy Policy, and that clearly defines the scope, nature and purpose of the processing, the type of Personal Data involved, the duration of processing and the terms and conditions on which the processor or sub-processor is to carry out such processing, as may be necessary from time to time

for the purposes of its engagement with us in connection with the Agreement, and consistent with the accountability principle under PIPEDA;

4.1.2 ensure that such contract requires the processor or sub-processor to implement appropriate technical and organisational measures to ensure the security and lawful processing of Personal Data, in line with the Safeguards Principle (Principle 4.7) under PIPEDA; and

4.1.3 remain fully liable for the acts or omissions of any processor or sub-processor in performing its data processing obligations under the Agreement, as if they were our own acts or omissions.

4.2 We will ensure that all persons authorised by us to process Personal Data on our behalf are bound by a duty of confidentiality, except where disclosure is required by Applicable Laws. In such cases, and where legally permitted and practicable, we will notify you of the legal requirement before disclosing such Personal Data. This obligation shall remain in effect even after the expiry or termination of our written contract with such processors or sub-processors.

4.3 We will maintain complete, accurate, and up-to-date written records of all processing activities carried out by us and by any processors or sub-processors we engage, including cross-border transfers, consistent with the accountability records required under PIPEDA and any applicable Canadian provincial privacy legislation.

5. RECORDS OF PROCESSING ACTIVITIES

We will maintain complete, accurate and up-to-date written records of all categories of processing activities carried out in accordance with the Data Protection Laws (the "Records").

6. PERSONAL DATA BREACHES

6.1 We will comply with our obligations under the Data Protection Laws to report any Personal Data Breach to the Office of the Privacy Commissioner of Canada ("OPC") and, where applicable, to affected individuals where the breach creates a real risk of significant harm in accordance with PIPEDA and any applicable Canadian provincial privacy legislation.

6.2 We will notify you as soon as reasonably possible upon becoming aware of any Personal Data Breach by us or otherwise in connection with our DXP Services. This notification will include all relevant details of the Personal Data Breach known at the time, and we will provide you with any updates thereafter.

6.3 We will provide you with reasonable cooperation and assistance as necessary to facilitate the handling of a Personal Data Breach in a timely and compliant manner and to enable us to comply with our obligations under the Data Protection Laws.

6.4 We will not issue or publish any filing, communication, notice, press release or report concerning any Personal Data Breach unless we are required to do so under the Data Protection Laws and/or by the OPC, any applicable Canadian provincial privacy commissioner or FINTRAC, in which case, we will notify you in advance of such requirement.

6.5 We will promptly and appropriately investigate any Personal Data Breach and to the best of our ability, identify, prevent and mitigate its effects. We will take reasonable steps to remedy any such breach as far as practicable.

6.6 We will keep you informed of any material developments relating to the Personal Data Breach. For Canadian Personal Data, we will also maintain a record of all security breaches (whether or not they create a real risk of significant harm) for at least 8 years from the date the breach is identified, in accordance with the PIPEDA Breach of Security Safeguards Regulations and our record retention policy, and make such records available to the OPC upon request.

7. YOUR OBLIGATIONS AS CONTROLLER OR JOINT CONTROLLER

7.1 Irrespective of whether we act as a joint controller, controller, or processor:

7.1.1 you are solely responsible for ensuring that the technical and organisational measures you implement are adequate and comply with the requirements of the Data Protection Laws and any other obligations you have under Applicable Laws;

7.1.2 you will comply, at all times, with your obligations as a controller or joint controller (as applicable) and will provide your services to clients in compliance with the Data Protection Laws;

7.1.3 you will maintain any valid registrations required by PIPEDA and any applicable Canadian provincial privacy legislation, and pay any fees as required by your Supervisory Authority to cover your processing activities, including those set out under the Agreement;

7.1.4 you will implement and maintain adequate data processing, privacy and IT security policies that govern your processing of Personal Data and response to any cybersecurity incidents, in compliance with Applicable Laws.

7.1.5 you shall ensure that both you and your personnel comply with these policies at all times and that your personnel are subject to written confidentiality obligations covering their processing of Personal Data. Where we consider certain control requirements not applicable to the DXP Services, we may agree to waive or modify them by giving you with written notice;

7.1.6 you shall provide all necessary, fair and transparent information and notices to, and obtain all required consents from, any Data Subjects whose Personal Data is processed under this Addendum, including your personnel, customers, and third parties, to ensure that we

may lawfully process such Personal Data for any Permitted Purpose, without the need for any further consent, approval or authorisation.

7.1.7 upon our reasonable request, you shall consult with us and comply with any reasonable directions we provide in relation to such notices and consents. These notices will include:

7.1.7.1 the purposes for which the Personal Data is being processed;

7.1.7.2 the legal justification for such processing;

7.1.7.3 the recipients of the Personal Data; and

7.1.7.4 any other information required under the Data Protection Laws;

7.1.8 if requested by us, you will promptly provide reasonable evidence that you have provided the necessary information and obtained all required consents from Data Subjects and otherwise complied with your obligations under the Data Protection Laws;

7.1.9 we will be entitled to assume that any disclosure or transfer of Personal Data to us by you (directly or indirectly) has been carried out in compliance with the Data Protection Laws;

7.1.10 you will ensure that any Personal Data you disclose or transfer to us is accurate;

7.1.11 you will not disclose or transfer any excessive or irrelevant Personal Data to us that is not required in connection with the performance of the DXP Services or any Permitted Purpose, and you will ensure that such data is removed from any documents before you provide them to us;

7.1.12 you will notify us promptly, within 48 (forty-eight) hours, if you become aware of a Personal Data Breach by us or in connection with the DXP Services. You will provide us with all the relevant details of the Personal Data Breach, known at the time, and keep us updated as further information becomes available;

7.1.13 you will provide us with reasonable cooperation and assistance as necessary to facilitate the handling of a Personal Data Breach in a timely and compliant manner and to enable us to comply with our obligations under the Data Protection Laws. You will not issue or publish any filing, communication, notice, press release or report concerning any Personal Data Breach involving us or in connection with the DXP Services, unless required to do so under the Data Protection Laws and/or by a Supervisory Authority, in which case, you will notify us in advance of such requirement;

7.1.14 you will notify us promptly (where legally permissible and within no more than 2 (two) business days) if you receive or become aware of any Data Complaint, whereafter you will provide reasonable cooperation and assistance as necessary to enable us to effectively address the Data Complaint;

7.1.15 you will provide us with reasonable cooperation and assistance as may be required to enable us to comply with our obligations under the Data Protection Laws, including those relating to security, Data Subject Requests, data protection impact assessments and consultations with a Supervisory Authority;

7.1.16 you shall comply with applicable data localisation, transfer, and retention requirements, including the cross-border transfer accountability requirements under PIPEDA and any applicable Canadian provincial privacy legislation

7.1.17 you shall facilitate the exercise of Data Subject rights under PIPEDA and any applicable Canadian provincial privacy legislation, including rights of access, correction, deletion, and objection, and cooperate with us in responding to such requests in a timely manner; and

7.1.18 you will comply with any additional obligations imposed on you in the other Parts of this Addendum.

8. DATA RETENTION

8.1 We will not retain Personal Data for longer than is necessary to carry out the Permitted Purposes.

8.2 We will maintain and comply with our data retention policy, details of which we will provide to you on written request.

9. REGULATORY COOPERATION

We acknowledge that the Office of the Privacy Commissioner of Canada ("OPC") is the federal authority responsible for overseeing compliance with PIPEDA, and that FINTRAC is the competent authority for anti-money-laundering supervision of our regulated activities in Canada. In this regard we will fully cooperate with FINTRAC, the OPC and any applicable Canadian provincial privacy commissioners in connection with the processing of Personal Data or any other virtual asset-related data.

10. LIABILITY EXCLUSIONS

10.1 To the extent permitted by law, any contractual liability caps applicable under the Agreement shall not apply to: (a) breaches of confidentiality; (b) breaches of data protection or information security obligations under this Addendum or the Data Protection Laws; (c) unlawful processing arising from failure to establish or maintain a lawful basis under the Data Protection Laws; or (d) any indemnification obligations set out in this Addendum or the Agreement.

10.2 Nothing in this Addendum shall limit either Party's liability for fraud, gross negligence, willful misconduct, or any liability that cannot lawfully be limited under the Applicable Laws.

DEUSXPAY

SECTION D

JOINT CONTROLLER TERMS

This Section applies where the parties jointly determine the purposes and means of processing Personal Data and agree to act as joint controllers under, or in connection with, the Agreement ("Joint Data") within the meaning of PIPEDA and any applicable Canadian provincial privacy legislation.

The Parties shall comply with the provisions set out in this Section D and with all the Data Protection Laws, in addition to the Technical and Organisational Measures set out in Section C of this Addendum.

1. PROCESSING OF JOINT DATA

1.1 Each Party will comply with its obligations as a controller under the Data Protection Laws in connection with its processing of Joint Data.

1.2 Each Party agrees that:

1.2.1 the Parties will jointly determine the purpose and means of processing the Joint Data, and will be jointly and individually responsible for ensuring there is a valid legal basis for processing the Joint Data under its control;

1.2.2 the Joint Data will be processed solely for a Permitted Purpose and within the scope of Schedule 1 to this Addendum, as updated from time to time;

1.2.3 the Joint Data will be collected, processed, and transferred in compliance with all the Data Protection Laws;

1.2.4 the Parties shall maintain accurate and up-to-date records of processing activities carried out in its capacity as a joint controller, consistent with the accountability principle under PIPEDA. These records, data processing facilities, systems, audit logs or any other relevant documentation necessary to demonstrate compliance with the Data Protection Laws, shall be made available to the OPC or any applicable Canadian provincial privacy commissioner upon request; and

1.2.5 each Party is responsible for providing all necessary, fair and transparent information and notices to Data Subjects. Such information must explain the processing of Joint Data for any Permitted Purpose, the legal basis for such processing, the recipients of the Joint Data (including the other Party, any third parties or regulators), and any other details required to be provided by a controller under the Data Protection Laws. All notices must disclose the arrangement between the Parties in compliance with the Data Protection Laws.

2. CO-OPERATION AND ASSISTANCE

2.1 The Parties shall co-operate in good faith and provide mutual assistance as reasonably necessary.

2.2 Each Party agrees:

2.2.1 to cooperate with the other Party and provide any information reasonably required to enable the other Party to prepare and publish the information and notices described in clause 1.2.5 of this Section D;

2.2.2 to cooperate with the other Party to ensure that Data Subjects can effectively exercise their rights under the Data Protection Laws, including rights of access, rectification, erasure, objection, restriction, and data portability;

2.2.3 to cooperate to ensure that the Security Measures are implemented and maintained to effectively protect the Joint Data;

2.2.4 to ensure that any Data Subject who wishes to make a Data Subject Request has an easily accessible point of contact to do so;

2.2.5 to provide reasonable assistance the other Party as required to ensure compliance with the other Party's obligations under Data Protection Laws with respect to security, Personal Data Breach notifications, data protection impact assessments and consultations with Supervisory Authorities, in so far as they relate to the processing of Joint Data; and

2.2.6 that it will promptly notify the other Party in writing upon receiving any formal request, inquiry, investigation notice, or other communication from the OPC, any applicable Canadian provincial privacy commissioner or FINTRAC, related to the Agreement or this Addendum, or the processing of Personal Data under the Agreement and this Addendum.

3. DATA SUBJECT REQUESTS AND DATA COMPLAINT HANDLING

3.1 If a Party receives a Data Subject Request or a Data Complaint relating to the processing of Joint Data, it will promptly notify the other Party in writing within 48 (forty-eight) hours of receipt and comply with the provisions of this Clause 3.

3.2 Between the Parties acting as joint controllers, responsibility for compliance with and responding to:

3.2.1 any Data Subject Request will fall on the Party that first received the request; and

3.2.2 any Data Complaint will fall on the Party that received the complaint;

unless otherwise agreed to by the Parties in writing.

3.3 Irrespective of who bears the responsibility of a Data Subject Request and/or a Data Complaint, both Parties will provide reasonable assistance to each other to assist with handling Data Subject Requests and Data Complaints relating to the processing of Joint Data.

3.4 Each Party will address any Data Subject Request or Data Complaint relating to the processing of Joint Data in a timely and professional manner and in accordance with the Data Protection Laws.

3.5 Neither party will respond to a Data Subject Request or Data Complaint without first consulting with the other Party, unless failing to respond would result in a breach of the Data Protection Laws or the Party is required to respond by the OPC, any applicable Canadian provincial privacy commissioner or any other Supervisory Authority.

3.6 Where a Data Subject Complaint cannot be resolved to the satisfaction of the Data Subject, the Parties shall inform the Data Subject of their right to escalate the matter to the Office of the Privacy Commissioner of Canada (OPC) or any applicable Canadian provincial privacy commissioner and provide reasonable assistance in facilitating such escalation.

3.7 Any Data Subject Requests and Data Complaints should be sent to security@deusxpay.com.

4. PERSONAL DATA BREACHES

4.1 If a Personal Data Breach occurs in relation to the Joint Data processed by either party:

4.1.1 Notification

The Party that discovers the Personal Data Breach will notify the other Party without undue delay (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 Data Subjects as soon as such information becomes available, and any other information that the other Party may reasonably request.

4.1.2 Co-operation

The Parties will cooperate in good faith to determine the cause of the Personal Data Breach, the scope and impact of the breach, and who should notify the OPC, any applicable Canadian provincial privacy commissioner and/or the affected Data Subjects (the "Notifying Party"), if required under the Data Protection Laws, as well as agree on the content and timing of any such notifications. In the absence of any agreement, we will be entitled to notify the OPC, any applicable Canadian provincial privacy commissioner and/or affected Data Subjects.

4.1.3 Communication with Supervisory Authorities and Data Subject(s)

The Notifying Party will be responsible for making any required notifications to the OPC, any applicable Canadian provincial privacy commissioner and/or affected Data Subjects. The other Party will provide all reasonable assistance to ensure timely and compliant notification to the OPC, any applicable Canadian provincial privacy commissioner and/or affected Data Subjects.

4.1.4 Rectification

The Party suffering the Personal Data Breach will take action immediately to carry out any recovery or other action necessary to remedy the Personal Data Breach.

4.2 Each Party will maintain appropriate records of any Personal Data Breach and the actions taken in response, consistent with the record-keeping requirements under the PIPEDA Breach of Security Safeguards Regulations. These records shall be made available to the OPC or any other competent Supervisory Authority upon request.

4.3 No Party will make any public statement, admission of fault, or communicate with the OPC, any applicable Canadian provincial privacy commissioner, FINTRAC or any other Supervisory Authority or Data Subjects regarding a breach involving jointly controlled data without the prior written agreement of the other Party, unless legally required to do so.

5. DATA PROCESSING OFFICER

If either party processes data on a scale, or in a manner, that triggers Data Processing Officer ("DPO") requirements under the Data Protection Laws, the Party shall designate a Privacy Officer accountable for compliance with PIPEDA and any applicable Canadian provincial privacy legislation. Each party shall provide the other with the contact details of its appointed DPO and co-operate to ensure a consistent approach to data protection compliance.

6. NO TRANSFER OF LIABILITY

Nothing in this Section D (Joint Controller Terms) shall be construed as transferring or limiting either Party's liability under Data Protection Laws for its own failure to comply with its obligations as a Joint Controller.

DEUSXPAY

SECTION E

CONTROLLER TERMS

This Section applies where we, as an Independent Controller, determine the purposes and means of processing Personal Data in connection with the Agreement ("Controller Data").

We will comply with the provisions set out in this Section E and with all the Data Protection Laws, in addition to the Technical and Organisational Measures in Section C of this Addendum.

1. PROCESSING CONTROLLER DATA

1.1 We will comply with our obligations as a controller in connection with our processing of Controller Data under the Data Protection Laws.

1.2 We will:

1.2.1 process the Controller Data solely for a Permitted Purpose and within the scope of Schedule 1 to this Addendum, as updated from time to time;

1.2.2 provide all necessary, fair, and transparent information and notices to Data Subjects, ensuring that such notices clearly explain the processing of Controller Data, the legal basis for processing, the recipients of the Controller Data (including any third parties or regulators), and any other information required to be provided by a controller under Data Protection Laws; and

1.2.3 ensure that any Data Subject who wishes to make a Data Subject Request in connection with Controller Data has an easily accessible point of contact to do so.

2. DATA SUBJECT REQUESTS

We, acting as the controller, will be solely responsible for handling any Data Subject Requests and Data Complaints in compliance with the Data Protection Laws. We will ensure that any Data Subject who wishes to make a Data Subject Request in connection with Controller Data has a clear, easily accessible, and user-friendly point of contact through which such requests can be submitted and acknowledged without undue delay.

DEUSXPAY

SECTION F

PROCESSOR TERMS

This Section applies where we process Personal Data as a processor on your behalf under, or in connection with the Agreement, within the meaning of PIPEDA and any applicable Canadian provincial privacy legislation.

We will comply with the provisions set out in this Section F and with all the Data Protection Laws, in addition to the Technical and Organisational Measures in Section C of this Addendum.

1. DETAILS OF PROCESSING

1.1 Insofar as we process Personal Data on your behalf, we shall:

1.1.1 unless required to do otherwise by Applicable Laws (and ensuring that any person acting under our authority does the same), process the Personal Data only in accordance with the Agreement, Schedule 1 to this Addendum, and any other documented instructions you provide ("Processing Instructions"); and

1.1.2 if Applicable Laws require us to process Personal Data other than in accordance with the Processing Instructions, notify you of that requirement before processing (unless prohibited from doing so by law on important grounds of public interest).

1.2 We will not process Personal Data for any purpose other than a Permitted Purpose, nor retain any Personal Data beyond the duration of the Agreement, unless required by Applicable Law.

2. PERSONNEL AND SUB-PROCESSORS

2.1 We will not engage any sub-processor to carry out any processing activities in respect of Personal Data without notifying you. This is subject to our compliance with clauses 2.2 and 2.3 of this Section F, and clause 4 of Section C. You will be deemed to have approved any proposed sub-processor if you do not object within 30 (thirty) calendar days of receiving our notice.

2.2 We shall:

2.2.1 provide you with details of any sub-processor;

2.2.2 notify you at least 30 (thirty) days in advance of any change, addition, or replacement of a sub-processor and provide sufficient information for you to decide whether to consent. You will be entitled to object to any such change and, at your discretion, may elect to terminate the Agreement or the relevant part of it if we do not take reasonable steps to address your objection and cease using the relevant sub-processor;

2.2.3 before any sub-processor carries out any processing activities in respect of the Personal Data, enter into a written contract with them that imposes obligations offering materially

the same level of protection for the Personal Data as those set out in this Addendum. This will include an obligation on the sub-processor to provide sufficient guarantees to implement technical and organisational security measures equivalent to the Security Measures outlined in clause 2 of Section C, and to delete or return the Personal Data in accordance with clause 7 of this Section F. The contract will also state that you may enforce compliance with these obligations if we cease to exist or become insolvent. At your request, we will provide you with a copy of the contract with any sub-processor. We may redact the text of the contract to the extent necessary to protect confidential information including any personal data belonging to the sub-processor; and

2.2.4 notify you of any failure by a sub-processor to fulfil its contractual obligations.

2.3 Where a sub-processor is located outside of Canada, or will process Personal Data outside Canada, we shall ensure that such transfer complies with the cross-border data transfer requirements of PIPEDA and any applicable Canadian provincial privacy legislation. We shall not permit transfers unless:

2.3.1 The destination country provides a comparable level of protection consistent with the accountability principle under PIPEDA;

2.3.2 Appropriate Safeguards are implemented; or

2.3.3 The Data Subject has provided explicit consent or another valid legal justification exists.

2.4 We shall ensure that sub-processors maintain appropriate security certifications (e.g., ISO/IEC 27001 or equivalent), undergo regular third-party audits, and are subject to compliance oversight to ensure conformity with technical and organisational security requirements.

2.5 We shall provide you, the OPC, any applicable Canadian provincial privacy commissioner or any other competent Supervisory Authority, with a list of sub-processors and relevant details upon request.

2.6 We will ensure that all persons authorised by us or any sub-processor to process Personal Data are bound by an obligation of confidentiality and will only access Personal Data on a "need-to-know" basis for the Permitted Purposes.

2.7 We will remain fully liable to you for any acts or omissions of any sub-processor, and of any persons authorised by us or any sub-processor to process Personal Data, as if they were our own acts or omissions.

3. TECHNICAL AND ORGANISATIONAL MEASURES

3.1 We will implement and maintain the Security Measures in accordance with clause 2 of Section C above, to:

3.1.1 ensure that the processing of Personal Data meets the minimum requirements under the Data Protection Laws, as specifically set out in PIPEDA and any applicable Canadian provincial privacy legislation, and ensure the protection of the rights of Data Subjects; and

3.1.2 provide reasonable assistance to you in responding to Data Subject Requests relating to Personal Data.

4. INFORMATION AND AUDIT

4.1 In accordance with the Data Protection Laws and subject to clause 4.2 of this Section F, we will, (as is reasonably necessary to remain compliant with our obligations under Section C, this Section F and the Data Protection Laws):

4.1.1 make available to you the Records, as soon as reasonably practicable, unless providing such information infringes the Data Protection Laws or any Applicable Law (in which case, we will inform you to the extent we are permitted by law to do so); and

4.1.2 allow for and contribute to audits, including inspections, by you (or an auditor mandated by you and approved by us in writing, for the purposes of verifying our compliance with this Addendum and applicable Data Protection Laws).

4.2 You agree to:

4.2.1 provide us with prior written notice (not less than 10 (ten) business days) of any information request, audit or inspection that you require, except where such audit is required by the OPC, any applicable Canadian provincial privacy commissioner, FINTRAC or any other Supervising Authority, or where a data breach or suspected data breach has occurred;

4.2.2 ensure that the Records and all information obtained or generated by you or your auditor in connection with such information requests, inspections and audits are kept strictly confidential, and not disclose same to any third party unless required to do so by the OPC, any applicable Canadian provincial privacy commissioner, FINTRAC or any other Supervising Authority, in which case, you will (to the extent legally permissible) provide us with no less than 14 (fourteen) days written notice of such requirement before such disclosure is given;

4.2.3 ensure that such audit or inspection is conducted during our normal business hours, with minimal disruption to our operations and those of our other customers;

4.2.4 bear your own costs associated with audits and reimburse us for our reasonable and documented internal costs incurred for assisting with the provision of information and allowing for and contributing to inspections and audits; and

4.2.5 comply with any additional obligations with regards to access by you or an auditor as set out in the Agreement.

4.3 Both Parties shall be entitled to share any information referred to in this clause 4 of this Section F, including the results of any audit, with the OPC, any applicable Canadian provincial privacy commissioner, FINTRAC or any other competent Supervisory Authority as may be necessary from time to time.

4.4 Nothing in clause 4 of this Section F entitles you to access any data belonging to our other customers, or any information that could cause us to breach our obligations under Data Protection Laws or our confidentiality obligations to any third Party.

5. ASSISTANCE WITH DATA SUBJECT RIGHTS

5.1 We are responsible for maintaining a record of Data Subject Requests. Upon receipt of any Data Subject Request, we shall immediately (within 48 (forty-eight) hours of receipt) refer such Data Subject Request to you and shall, at our own expense, promptly assist you with such Data Subject Request to ensure that you meet the response times under the Data Protection Laws.

5.2 We will not respond to a Data Subject Request without providing prior written notice to you or as required by Applicable Laws, in which case we shall, to the extent permitted by Applicable Laws, inform you of that legal requirement prior to us responding to such Data Subject Request.

5.3 We will provide such assistance as reasonably required by you to ensure compliance with your obligations under the Data Protection Laws with respect to:

5.3.1 security of processing;

5.3.2 data protection impact assessments (as defined in the Data Protection Laws);

5.3.3 prior consultation with the OPC and/or any applicable Canadian provincial privacy commissioner regarding any high-risk processing;

5.3.4 notifications to the OPC, any applicable Canadian provincial privacy commissioner or any other Supervisory Authority and/or communications to Data Subjects in response to any Personal Data Breach; and

5.3.5 any remedial action to be taken in response to a Personal Data Breach and/or a Data Complaint or request relating to your obligations under the Data Protection Laws relevant to the Agreement.

6. BREACH NOTIFICATION

6.1 In respect of any Personal Data Breach, we will, without undue delay and no later than 48 (forty-eight) hours (or earlier where possible) after becoming aware, notify you of the Personal Data Breach and provide you with details known at the time of the Personal Data Breach, including the nature of the Personal Data Breach, the categories and approximate volume of Data Subjects, the Personal Data concerned, the likely consequences of the Personal Data Breach and any measures taken or to be taken by us to mitigate the effects of the Personal Data Breach.

6.2 We will provide you with further information as and when it becomes available to us and without undue delay (no later than 24 (twenty-four) hours after becoming aware of the new information).

6.3 We will immediately, at our own expense, investigate the Personal Data Breach and take steps to identify, prevent and mitigate the effects of and to remedy any Personal Data Breach. We will not release or publish any filing, communication, notice, press release or report concerning any Personal Data Breach without your prior written approval.

6.4 We will promptly (no later than 48 (forty-eight) hours after becoming aware) inform you if we receive or become aware of a Data Complaint and shall not respond to the Data Complaint without your prior written approval.

7. DELETION OR RETURN OF PERSONAL DATA AND COPIES

7.1 We will process the Personal Data only for the duration of the Data Processing Term.

7.2 At your written request, we will ensure that any Personal Data (and all copies) are securely returned to you or destroyed (at your discretion and direction) to the extent reasonably practicable (unless storage is required by Applicable Laws and, if so, we will inform you of any such requirement) in the following circumstances:

7.2.1 on termination of the Agreement;

7.2.2 on expiry of the Data Processing Term; and/or

7.2.3 once processing of the Personal Data is no longer necessary for the Permitted Purposes.

DEUSXPAY

SCHEDULE 1 – DETAILS OF PERSONAL DATA

Category of Personal Data collected	**Type of Personal Data collected**
1.) Identifiers	• Full name; • Date of birth; • Nationality; • Gender; • Government-issued identification (passport number, Canadian federal or provincial identification such as driver's licence or provincial ID card, Social Insurance Number where lawfully required); • Photographs or biometric data (e.g., facial recognition, fingerprints) for identity verification; and • Signature.
2.) Contact Data	• Email address; • Phone number; • Residential or mailing address; • Billing address; • Social media handles or usernames (if applicable);
3.) Professional or Employment-Related information	• Job title; • Company name; • Company registration number; and • Education background.
4.) Financial and Transaction Data	• Account details; • Wallet details; • Source of funds; • Credit information; • Account Authentication details; • Transaction history; and • Payment method details.
5.) Technical and Usage Data	• IP address; • Device information (e.g., device ID, operating system, browser type);

	• Log-in data (usernames and passwords) and session activity; • Two-factor authentication information; • Security questions and answers; • Location, time zone and geological data (where permitted); • Details of services assessed and platform usages; • Virtual asset transaction data, including wallet addresses and transaction amounts; and • Logs of user activity on the platform.
6.) KYC and Compliance Data	• Background check information (e.g., sanctions screening, PEP status); • Responses to KYC/AML questionnaires; • Proof of identity and proof of address; and • Risk profiling and due diligence reports.
7.) Communication Data	• Information provided in email correspondence, recorded calls, chat logs, or face-to-face meetings (including Zoom/Microsoft Teams online meetings); • Customers support interactions; • Notes or records from onboarding interviews or compliance meetings; and • Feedback or survey responses.
8.) Marketing and Preferences Data	• Your preferences in receiving marketing communications; and • Data on how you interact with our communications and website content.
9.) Legal	• Legal documents and Agreements entered into between you and us.

DEUSXPAY

SENSITIVE PERSONAL DATA

The following categories of Personal Data constitute Sensitive Personal Data and are subject to safeguards proportionate to sensitivity under Principle 4.7 (Safeguards) of PIPEDA and any applicable Canadian provincial privacy legislation:

Category of Sensitive Personal Data	**Type of Sensitive Personal Data collected**
Government-issued Identification	Passport number; Canadian driver's licence; provincial identity card details; Social Insurance Number where lawfully required.
Biometric Data	Facial recognition data; fingerprints; liveness verification data collected for identity verification (including via Sumsub).
AML / Sanctions Screening Outcomes	Sanctions match results; PEP status; adverse media findings; criminal-related screening hits.
Authentication Credentials	Account log-in credentials; two-factor authentication data; security questions and answers; session tokens.
Financial Account Identifiers	Bank account numbers; cardholder data (PANs); cryptocurrency wallet addresses linked to an identifiable natural person.
Source of Funds / Source of Wealth	Banking statements; sales or other contracts; further documentation collected during Enhanced Due Diligence to evidence the source of funds or source of wealth.

DEUSXPAY

SCHEDULE 2 – CROSS BORDER TRANSFER MECHANISMS

1. DEFINITIONS

1.1 Terms used in this Schedule 2 shall have the meanings set out below, in the Addendum, or as otherwise defined in PIPEDA and any applicable guidance issued by the OPC or any applicable Canadian provincial privacy commissioner.

1.1.1 **"Cross-Border Transfer"** means any disclosure, transmission, access to, or processing of Personal Data by a party located in a jurisdiction outside Canada, whether directly or through onward transfer; and

1.1.2 **"Adequate Jurisdiction"** means any country or territory deemed by the Office of the Privacy Commissioner of Canada (OPC), or any applicable Canadian provincial privacy commissioner, to offer comparable protection consistent with the PIPEDA accountability principle, as set out in its published adequacy list of guidance.

2. CROSS BORDER DATA TRANSFER MECHANISMS

2.1 Legal Basis for Cross-Border Transfers

2.1.1 The transfer of Personal Data to any entity or recipient located outside Canada shall only be permitted if:

2.1.1.1 the recipient is located in an Adequate Jurisdiction as recognised by the OPC or any applicable Canadian provincial privacy commissioner; or

2.1.1.2 where the recipient is located in a jurisdiction not recognised as adequate, the transfer is subject to:

2.1.1.2.1 appropriate contractual or organisational safeguards that ensure an adequate level of protection for the Personal Data, including:

- data transfer agreements incorporating PIPEDA-compliant clauses (including, where applicable, the Model Contract Clauses recognised under Quebec's Law 25);
- binding intra-group data transfer policies; and
- other legally recognised safeguards consistent with PIPEDA and any applicable Canadian provincial privacy legislation;

2.1.1.2.2 one of the limited derogations recognised under PIPEDA and applicable Canadian provincial privacy legislation, including:

- the explicit and informed consent of the Data Subject;
- the necessity of the transfer for the performance of a contract;

- compliance with legal or judicial obligations;
- protection of public interest or public health; and
- establishment, exercise, or defence of legal claims.

2.2 Notification and Record-Keeping Requirements

2.2.1 Each party shall:

2.2.1.1 Maintain records of all cross-border transfers conducted under the Agreement and this Addendum, including:

2.2.1.1.1 the categories of Personal Data transferred;

2.2.1.1.2 the identity and location of the data importer; and

2.2.1.1.3 the applicable safeguard or legal basis relied upon.

2.2.2 Provide such records to the OPC, any applicable Canadian provincial privacy commissioner, FINTRAC or any other Supervisory Authority, upon request.

2.3 Supervisory Authority and Cooperation

2.3.1 Each party agrees to:

2.3.1.1 cooperate fully with any investigation, inquiry, audit or assessment initiated by the OPC, any applicable Canadian provincial privacy commissioner, FINTRAC or any other Supervisory Authority in relation to cross-border transfers; and

2.3.1.2 promptly notify the other party if it receives a request, complaint, or directive from a Supervisory Authority related to any cross-border transfer conducted under this Agreement and/or Addendum.

2.4 Changes in Law

2.4.1 If, following the effective date of this Addendum, the legal framework governing Cross-Border Transfers in Canada is amended or updated, or new requirements are imposed by the OPC, any applicable Canadian provincial privacy commissioner or FINTRAC, the parties shall:

2.4.1.1 promptly review and update their cross-border data transfer arrangements to ensure compliance; and

2.4.1.2 negotiate in good faith to implement any new contractual terms or safeguard mechanisms necessary for continued compliance with applicable Data Protection Laws.

2.5 Conflict

In the event of any conflict between this Schedule 2 and any other provision of this Addendum or the Agreement, the provisions of this Schedule 2 shall prevail to the extent necessary to comply with applicable Canadian Data Protection Laws and regulatory requirements.

DEUSXPAY

SCHEDULE 3

SUB-PROCESSORS

Third Party Sub-Processor	Applicable Service(s)	Purpose of Processing	Location of Processing
Google Workspace Enterprise Plus	Data and Application Hosting Provider, including Email and Document Management	Infrastructure/Cloud Provider	USA/Global
Copper CRM	Customer Relationship Management and Sales Pipeline Management	CRM and Customer Data Management	USA
Microsoft 365 (Teams)	Communication and Collaboration Platform	Internal Communication and Collaboration	USA/Global
Xero	Accounting and Financial Management Software	Legal and Regulatory Bookkeeping and Accounting	UK & USA
Refinitiv (LSEG)	Financial Data and Analytics Services	Financial Data Provider and Market Intelligence	UK/Global
Zapier	Workflow Automation and Integration Platform	Integration and Automation Services	USA
Jira (Atlassian)	Project Management and Issue Tracking	Project Management and Development Operations	USA
Cloudflare	Web Security and Performance Services	Security, CDN and Web Performance	USA/Global
Amazon Web Services (AWS)	Cloud Infrastructure and Computing Services	Infrastructure / Cloud Provider	USA/Global

Slack	Communication and Collaboration Platform	Internal Communication and File Sharing	USA
DXP Affiliated Entities	Various business support services	Group Services and Operations	Canada, UK
Apollo	Lead Enrichment and Data Accuracy Services	Verification, supplementation, and enrichment of lead and prospect data (with consent)	USA/Global
Sumsub (Sum and Substance Ltd)	Onboarding and Identity Verification Platform	KYC, KYB, AML and Sanctions Screening, Enhanced Due Diligence (EDD), Liveness and Biometric Verification	UK / EU / Canada
Fireblocks Ltd	Digital Asset Custody and Wallet Infrastructure	Virtual asset custody, wallet management, transaction signing and cryptographic key management for client virtual asset holdings	USA / EU / Canada
Elliptic Enterprises Ltd	Blockchain Analytics and On-Chain Transaction Monitoring	AML / CFT analytics, sanctions screening of wallet addresses, transaction risk scoring, and detection of suspicious on-chain activity	UK / USA / Global
Chainalysis Inc.	Blockchain Analytics and On-Chain Transaction Monitoring	AML / CFT analytics, sanctions screening of wallet addresses, transaction risk scoring, and	USA / EU

		detection of suspicious on-chain activity	
DocuSign, Inc.	Electronic Signature and Contract Lifecycle Management	Preparation, secure electronic signature, storage and audit trail of client, counterparty, employee and vendor agreements	USA / Global
Merkle Science Inc.	Blockchain Analytics and On-Chain Transaction Monitoring	Blockchain analytics, on-chain risk scoring, wallet screening and detection of illicit-finance exposure across virtual asset transactions	USA / Global
jQuery / StackPath (code.jquery.com CDN)	Third-Party JavaScript Content Delivery Network	Delivery of the jQuery JavaScript library referenced by the marketing website (no personal data is collected by the CDN beyond standard network metadata)	USA / Global
HubSpot, Inc.	Marketing File Hosting / Content Delivery	Hosting and delivery of publicly linked legal documents (Privacy Policy, Terms & Conditions, Risk Statement) served from the website footer	EU (HubSpot eu1 region)
ACX	Regulatory and AML Advisory Services	Regulatory advisory, AML programme assurance and independent attestation support	UK / EU

CryptoSwift OÜ	Virtual Asset Travel Rule Compliance Solution	Travel Rule messaging: originator/beneficiary data transmission between Virtual Asset Service Providers to satisfy FATF Recommendation 16 and equivalent Canadian obligations	Estonia / EU