DATA PROTECTION AGREEMENT

(Data Processing Addendum)

Between

BITHARBOUR LTD.

and

THE CUSTOMER

Version 1.0

A SpendLayer Group Company

Table of Contents

Parties and Background

This Data Protection Agreement ("DPA" or "Agreement") forms part of and is incorporated into the Principal Agreement (as defined below) between:

Processor	BITHARBOUR LTD., a corporation incorporated under the Business Corporations Act (Ontario), Ontario Corporation No. 1001339518, registered with FINTRAC as a Money Services Business under Registration No. C10001222, with its registered office at 200–5700 Yonge Street, North York, Ontario, M2M 4K2, Canada ("BitHarbour," "Processor," "we" or "us").
Controller	The customer, client or counterparty identified in the Principal Agreement that determines the purposes and means of processing Personal Data (the "Customer," "Controller" or "you").

BitHarbour and the Customer are each a "Party" and together the "Parties."

Recitals

A. BitHarbour is a FINTRAC-registered Money Services Business providing foreign exchange, virtual currency, money transfer, money order, payment (PSP) and cheque-cashing services under FINTRAC Registration No. C10001222.

B. The Customer has engaged BitHarbour to provide one or more of those services under a separate services, merchant, partnership or subscription agreement (the **"Principal Agreement"**).

C. In the course of providing those services, BitHarbour may Process Personal Data on behalf of the Customer. This DPA sets out the terms on which such Processing is carried out and governs the Parties' respective obligations under Data Protection Laws.

D. The Parties acknowledge that, in relation to Personal Data that BitHarbour is required to collect, verify, retain and report to satisfy its own legal and regulatory obligations (including anti-money laundering, counter-terrorist financing, sanctions screening and Know-Your-Customer obligations under Canadian federal law), BitHarbour acts as an **independent Controller** and not as a Processor, as further described in Clause 3.

In consideration of the mutual covenants below, the Parties agree as follows.

1. Definitions and Interpretation

1.1 Capitalised terms used but not defined in this DPA have the meaning given in the Principal Agreement. The following definitions apply:

"Data Protection Laws" means all laws and regulations applicable to the Processing of Personal Data under this DPA, including, as applicable: (a) the Personal Information Protection and Electronic Documents Act (Canada) ("PIPEDA") and any substantially similar provincial legislation; (b) Regulation (EU) 2016/679 (the "EU GDPR"); (c) the EU GDPR as incorporated into United Kingdom law by the Data Protection Act 2018 and the European Union (Withdrawal) Act 2018 (the "UK GDPR"); and (d) any implementing, successor or related legislation, in each case as amended or replaced from time to time.

"Controller" means the natural or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. Under PIPEDA, this corresponds to the organisation with primary responsibility for the Personal Data.

"Processor" means a natural or legal person that Processes Personal Data on behalf of the Controller. Under PIPEDA, this corresponds to a third party engaged to process Personal Data on behalf of the responsible organisation.

"Personal Data" means any information relating to an identified or identifiable natural person that is Processed by BitHarbour on behalf of the Customer under the Principal Agreement. It includes "personal information" as defined in PIPEDA and "personal data" as defined in the GDPR.

"Special Categories of Personal Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

"Data Subject" means the identified or identifiable natural person to whom Personal Data relates.

"Processing" (and "Process" and "Processed") means any operation performed on Personal Data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, dissemination, restriction, erasure or destruction.

"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 Processed under this DPA.

"Sub-processor" means any third party engaged by BitHarbour to Process Personal Data on behalf of the Customer.

"Standard Contractual Clauses" or "SCCs" means (a) for transfers subject to the EU GDPR, the standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914; and (b) for transfers subject to the UK GDPR, the International Data Transfer Addendum issued by the UK Information Commissioner, in each case as amended or replaced.

"Supervisory Authority" means (a) in Canada, the Office of the Privacy Commissioner of Canada or the relevant provincial privacy commissioner; and (b) in the EU/UK, the competent data protection authority.

1.2 The Annexes form an integral part of this DPA. In the event of conflict between the body of this DPA and an Annex, the body prevails unless the Annex expressly states otherwise. In the event of conflict between this DPA and the Principal Agreement in respect of the Processing of Personal Data, this DPA prevails.

2. Scope and Roles of the Parties

2.1 This DPA applies to the Processing of Personal Data by BitHarbour on behalf of the Customer under the Principal Agreement, where BitHarbour acts as a Processor.

2.2 The Customer, as Controller, determines the purposes and means of the Processing carried out on its behalf and warrants that it has a valid legal basis (and, where required, has obtained the necessary consents) for the Processing and for BitHarbour's Processing of the Personal Data as instructed.

2.3 The subject-matter, duration, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects are set out in **Annex 1**.

2.4 Each Party shall comply with its respective obligations under the Data Protection Laws in relation to the Processing.

3. BitHarbour as Independent Controller for Regulatory Compliance

3.1 Notwithstanding anything to the contrary, the Parties acknowledge that BitHarbour independently determines the purposes and means of Processing certain Personal Data in order to comply with legal and regulatory obligations to which it is directly subject, including under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (Canada) and its regulations, and requirements imposed by FINTRAC. In respect of such Processing, BitHarbour acts as an **independent Controller**.

3.2 This independent-Controller Processing includes, without limitation:

- verifying the identity of Data Subjects and conducting Know-Your-Customer and customer due-diligence procedures;
- screening Data Subjects and transactions against sanctions, politically-exposed-person and watch lists;
- monitoring, recording and reporting large cash, electronic funds, virtual currency and suspicious transactions to FINTRAC;
- retaining records for the periods required by applicable law; and
- responding to lawful requests, orders and production demands from FINTRAC, law-enforcement, courts and other competent authorities.

3.3 When acting as an independent Controller, BitHarbour is solely responsible for its compliance with Data Protection Laws in respect of that Processing, and the Processor obligations in Clauses 4 to 12 do not apply to it. The Customer shall not instruct or purport to instruct BitHarbour in relation to such Processing, and BitHarbour is not required to delete or return such Personal Data where retention is required by law.

4. Obligations of BitHarbour as Processor

Where and to the extent BitHarbour acts as a Processor, BitHarbour shall:

4.1 **Instructions.** Process the Personal Data only on documented instructions from the Customer, including as set out in this DPA and the Principal Agreement, unless required to do otherwise by applicable law; in which case BitHarbour shall, where legally permitted, inform the Customer of that legal requirement before Processing.

4.2 **Unlawful instructions.** Immediately inform the Customer if, in its opinion, an instruction infringes Data Protection Laws (without obligation to actively monitor the Customer's compliance).

4.3 **Confidentiality.** Ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and limit access to those personnel who need it to provide the services.

4.4 **Security.** Implement and maintain the technical and organisational security measures set out in **Annex 2** and in Clause 5.

4.5 **Assistance.** Taking into account the nature of the Processing, assist the Customer by appropriate technical and organisational measures, insofar as reasonably possible, to respond to requests from Data Subjects and to fulfil the Customer's obligations relating to security, breach notification, data protection impact assessments and prior consultation with Supervisory Authorities.

4.6 **Purpose limitation.** Not Process the Personal Data for any purpose other than performing the services or as otherwise instructed by the Customer, and not sell the Personal Data or use it for its own independent commercial purposes (save as permitted under Clause 3).

5. Security of Processing

5.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk to Data Subjects, BitHarbour shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as set out in **Annex 2**.

5.2 Such measures include, as appropriate: pseudonymisation and encryption of Personal Data; measures to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems; the ability to restore availability and access in a timely manner after an incident; and a process for regularly testing and evaluating the effectiveness of the measures.

5.3 BitHarbour shall maintain safeguards commensurate with the sensitivity of the Personal Data, consistent with its obligations under PIPEDA and its regulatory obligations as a FINTRAC-registered Money Services Business.

6. Sub-processors

6.1 The Customer grants BitHarbour general authorisation to engage Sub-processors to Process the Personal Data, subject to this Clause 6. A current list of Sub-processors is set out in **Annex 3**.

6.2 BitHarbour shall impose on each Sub-processor, by written contract, data-protection obligations that are no less protective than those in this DPA, and remains fully liable to the Customer for the performance of each Sub-processor's obligations.

6.3 BitHarbour shall give the Customer reasonable prior notice of any intended addition or replacement of a Sub-processor, and the Customer may object on reasonable data-protection grounds within fifteen (15) days. If the Parties cannot resolve the objection, the Customer may terminate the affected services under the Principal Agreement.

7. Data Subject Rights

7.1 BitHarbour shall, taking into account the nature of the Processing, assist the Customer by appropriate technical and organisational measures, insofar as reasonably possible, in fulfilling

the Customer's obligation to respond to requests by Data Subjects to exercise their rights, including rights of access, correction, deletion, restriction, portability and objection under applicable Data Protection Laws.

7.2 If BitHarbour receives a request directly from a Data Subject relating to Personal Data Processed on behalf of the Customer, it shall (unless legally prohibited) promptly forward the request to the Customer and shall not respond substantively except on the Customer's documented instructions or as required by law.

8. Personal Data Breach Notification

8.1 BitHarbour shall notify the Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Personal Data Processed on behalf of the Customer.

8.2 The notification shall, to the extent known, describe the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed to address the breach, and a contact point for further information. Where information is not available at once, it may be provided in phases without undue further delay.

8.3 BitHarbour shall take reasonable steps to mitigate the effects of, and to minimise any damage resulting from, the Personal Data Breach, and shall reasonably cooperate with the Customer in respect of any notification to Supervisory Authorities or Data Subjects. Notification of a breach is not, of itself, an acknowledgement of fault or liability.

9. International Data Transfers

9.1 BitHarbour Processes Personal Data primarily in Canada. Canada benefits from a partial adequacy decision of the European Commission in respect of commercial organisations subject to PIPEDA, which supports transfers of Personal Data from the European Economic Area to BitHarbour.

9.2 Where Personal Data subject to the EU GDPR or UK GDPR is transferred to a country that is not the subject of an adequacy decision, or where an adequacy decision does not apply, the Parties shall enter into and comply with the applicable **Standard Contractual Clauses**, which are incorporated into this DPA by reference and completed as set out in **Annex 4**. In case of conflict between the SCCs and this DPA, the SCCs prevail in respect of the relevant transfer.

9.3 Where required, BitHarbour shall assist the Customer in carrying out a transfer impact assessment and shall implement supplementary measures reasonably necessary to protect the transferred Personal Data.

10. Records and Audit

10.1 BitHarbour shall maintain records of its Processing activities carried out on behalf of the Customer as required by Data Protection Laws and make available to the Customer information reasonably necessary to demonstrate compliance with this DPA.

10.2 The Customer may, on at least thirty (30) days' prior written notice and no more than once in any twelve-month period (unless required by a Supervisory Authority or following a Personal

Data Breach), audit BitHarbour's compliance with this DPA. Audits shall be conducted during normal business hours, subject to reasonable confidentiality and security requirements, and in a manner that does not disrupt BitHarbour's operations or compromise the confidentiality of other customers' data or BitHarbour's regulatory obligations.

10.3 BitHarbour may satisfy an audit request by providing a recent independent third-party audit report or certification where such report reasonably addresses the matters in question.

11. Return and Deletion of Personal Data

11.1 On termination or expiry of the Principal Agreement, or on the Customer's written request, BitHarbour shall, at the Customer's choice, return or securely delete the Personal Data Processed on behalf of the Customer, and delete existing copies, unless retention is required by applicable law.

11.2 The Parties acknowledge that BitHarbour is required by anti-money-laundering, counter-terrorist-financing and other laws to retain certain records (including identity, transaction and reporting records) for prescribed periods. BitHarbour may retain such Personal Data as an independent Controller under Clause 3 for as long as required by law, after which it shall be securely deleted or anonymised.

12. PIPEDA-Specific Provisions

12.1 The Parties shall handle Personal Data in a manner consistent with the fair information principles in Schedule 1 to PIPEDA, including accountability, limiting collection, limiting use, disclosure and retention, accuracy, safeguards and openness.

12.2 Each Party remains accountable for Personal Data in its custody or control, including Personal Data transferred to a third party for Processing, and shall use contractual or other means to provide a comparable level of protection while the information is being Processed by that third party.

12.3 The Parties acknowledge that transferring Personal Data to a jurisdiction outside Canada may make it subject to the laws of that jurisdiction, and shall, where required, be transparent with Data Subjects about such transfers.

13. Term, Liability and General

13.1 **Term.** This DPA takes effect on the effective date of the Principal Agreement and continues for as long as BitHarbour Processes Personal Data on behalf of the Customer, and thereafter to the extent of any surviving obligations (including retention and confidentiality).

13.2 **Liability.** Each Party's liability arising out of or in connection with this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement.

13.3 **Governing law.** This DPA is governed by the laws of the Province of Ontario and the federal laws of Canada applicable therein, except where the Data Protection Laws of another jurisdiction mandatorily apply, and without prejudice to the governing law of any incorporated Standard Contractual Clauses.

13.4 **Severability.** If any provision of this DPA is held invalid or unenforceable, the remaining provisions continue in full force and effect.

13.5 **Entire agreement.** This DPA, together with the Principal Agreement and its Annexes, constitutes the entire agreement between the Parties in respect of the Processing of Personal Data and supersedes any prior arrangements on that subject-matter.

Signatures

Agreed and accepted by the duly authorised representatives of the Parties.

For and on behalf of BITHARBOUR LTD.

Signature: _____

Name: _____

Title: _____

Date: _____

For and on behalf of THE CUSTOMER

Signature: _____

Name: _____

Title: _____

Date: _____

Annex 1 – Details of Processing

Controller	The Customer identified in the Principal Agreement.
Processor	BitHarbour Ltd. (FINTRAC MSB No. C10001222).
Subject-matter	Provision of foreign exchange, money transfer, money order, virtual currency, payment (PSP) and/or cheque-cashing services under the Principal Agreement.
Duration	For the term of the Principal Agreement and any legally required retention period thereafter.
Nature and purpose	Collection, verification, storage, use, transmission and disclosure of Personal Data as necessary to onboard Data Subjects, execute and settle transactions, provide customer support, and meet contractual and regulatory obligations.
Categories of Data Subjects	The Customer’s customers, end-users, payees, beneficiaries, authorised representatives and employees whose Personal Data is provided to BitHarbour.
Types of Personal Data	Identification data (name, date of birth, nationality); contact data (address, email, telephone); government-issued identifiers and identity-document details; financial and transaction data (account details, payment instructions, amounts, currencies); device and log data; and any other data provided by the Customer.
Special Categories	Not intended to be Processed. The Customer shall not provide Special Categories of Personal Data except where strictly necessary and lawfully permitted.
Frequency of transfer	Continuous / on an ongoing basis for the duration of the services.

Annex 2 – Technical and Organisational Security Measures

BitHarbour maintains, at a minimum, the following measures, which may be updated provided the level of security is not materially reduced:

- Access control: role-based access, least-privilege principles, unique user credentials, and multi-factor authentication for administrative and remote access.
- Encryption: encryption of Personal Data in transit (TLS) and at rest using industry-standard algorithms.
- Network security: firewalls, segmentation, intrusion detection/prevention, and regular vulnerability scanning.
- Pseudonymisation and minimisation: limiting Personal Data to what is necessary and applying pseudonymisation where practicable.
- Confidentiality: confidentiality obligations for personnel and regular data-protection and AML/ATF training.
- Availability and resilience: backups, disaster-recovery arrangements, and procedures to restore access following an incident.
- Logging and monitoring: audit logging of access to and Processing of Personal Data.
- Incident management: a documented Personal Data Breach response and escalation process.
- Vendor management: due diligence and contractual controls over Sub-processors.
- Physical security: controlled access to premises and facilities where Personal Data is Processed.

Annex 3 – Approved Sub-processors

As at the effective date, BitHarbour engages the following Sub-processors. This list is updated in accordance with Clause 6, and the Customer will be given prior notice of any addition or replacement.

Sub-processor / Category	Processing Activity	Location
DigitalOcean (cloud hosting / infrastructure)	Hosting and storage of application data	United Kingdom
RiskScreen (identity verification / KYC)	Identity and document verification	United Kingdom / EU
LexisNexis (sanctions & PEP screening)	Watch-list and sanctions screening	United Kingdom / EU
Simplewealth AG (banking partner — SpendLayer Group company)	Execution and settlement of transactions	Switzerland
LedgerLink SA (banking partner — SpendLayer Group company)	Execution and settlement of transactions	Switzerland
Cublox Ltd. (third-party banking provider)	Execution and settlement of transactions (prospective; the Customer will be notified before this provider is engaged)	United Kingdom
Communications / support platform	Not applicable	—

Annex 4 – Standard Contractual Clauses (Transfer Mechanism)

Where Clause 9 requires the use of Standard Contractual Clauses, they are completed as follows:

Module	Module Two (Controller to Processor). Module Three (Processor to Processor) applies to onward transfers to Sub-processors.
Clause 7 (Docking clause)	Applies.
Clause 9 (Sub-processors)	Option 2 (General written authorisation), with the notice period set out in Clause 6.3 of this DPA.
Clause 11 (Redress)	The optional independent dispute-resolution provision does not apply.
Clause 17 (Governing law)	The law of the EU Member State in which the data exporter is established, or (where the exporter is outside the EU) the Republic of Ireland.
Clause 18 (Forum and jurisdiction)	The courts of the EU Member State identified under Clause 17.
Data exporter	The Customer (Controller).
Data importer	BitHarbour Ltd. (Processor).
Annex I / II / III of the SCCs	Populated by reference to Annexes 1, 2 and 3 of this DPA.
UK transfers	The UK International Data Transfer Addendum applies, with Tables 1–4 completed by reference to the above and this DPA; the version of the EU SCCs is the approved version referenced in Clause 1.1.