DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT ("DPA") is entered into as of the date of the Order Form (the "Effective Date").

BETWEEN:

Tulip.io, Inc., a Canadian corporation whose registered office is at 5 Michael St., Suite 201, Kitchener, ON, Canada N2G 1L7 ("**Processor**"); and Customer who is named and whose details are provided on the Order Form ("**Controller**").

RECITALS:

WHEREAS:

(A) Controller intends to transfer certain personal data to Processor, so that it may be Processed in accordance with the Master Services Agreement for the provision of Processor's services entered into by and between the parties on the date of the relevant Order Form (the "**Agreement**").
(B) The parties agree that this DPA will govern the parties' rights and obligations with respect to the processing of such personal data.

NOW IT IS AGREED as follows:

1. Data Protection

1.1. *Definitions:* In this DPA, the following terms shall have the following meanings:

(a) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in Applicable Data Protection Laws;

(b) "**Applicable Data Protection Laws**" means all worldwide data protection and privacy laws and regulations, to the extent applicable from time to time to the parties and the nature of the personal data processed under the Agreement, including, where applicable, (i) EU/UK Data Protection Law; (ii) the Canadian Personal Information Protection and Electronic Documents Act 2000 and applicable provincial laws ("PIPEDA"); (iii) the California Consumer Privacy Act (the "**CCPA**") as updated by the California Privacy Rights Act ("CPRA"); (iv) any federal and/or state privacy laws and regulations of the United States of America; and (v) any other applicable privacy laws.

(c) "**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

(d) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018;

(e) "**Security Incident"** means an actual unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

(f) "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, the international data transfer agreement for international data transfers, or the addendum to the EU SCCs, which came into force on 21 March 2022 and which can be used as a transfer tool to comply with Article 46 of the UK GDPR and which are made available by the Information Commissioner's Office ("**UK SCCs**").

1.2. *Relationship of the parties:* Controller instructs Processor to process the personal data that is the subject of the Agreement (the "**Data**") on its behalf. In respect of such processing, Controller shall be the controller and Processor shall be a processor. Each party shall comply with the obligations that apply to it under Applicable Data Protection Laws. Controller represents and warrants that it has provided all necessary and/or legally required notices and collected all necessary and/or legally required consents with respect to the Data, and that Processor's processing of the personal data will not infringe any third party rights or any applicable laws, including Applicable Data Protection Laws. Controller will indemnify and hold harmless Processor from any and all claims relating to the Data, except to the extent such claims are directly caused by Processor's gross negligence, willful misconduct, or material breach of this DPA.

1.3. *Purpose limitation:* Processor shall process the Data solely for the purposes described in Annex I and in accordance with Controller's documented instructions (the "Permitted Purpose"), provided that such instructions are lawful and do not conflict with Applicable Data Protection Law. Where Processor is required to process Data by laws to which it is subject, Processor shall, to the extent legally permitted, inform Controller of such legal requirement before processing. Notwithstanding the foregoing, Processor may process Data to the extent necessary for:

- providing the Services under the Agreement;
- ensuring system security, integrity, and availability;
- maintaining backups for disaster recovery purposes;
- complying with legal obligations, court orders, or regulatory requirements;
- protecting Processor's legitimate interests in defending legal claims; and
- aggregating Data in anonymized form for operational analytics, provided such anonymization renders the data non-personal under Applicable Data Protection Laws.

Controller warrants that its processing instructions are lawful and compliant with Applicable Data Protection Laws. Processor has no obligation to actively monitor Controller's compliance with Applicable Data Protection Laws or the lawfulness of Controller's instructions. If Processor becomes actually aware (without active monitoring) that Controller's instructions infringe Applicable Data Protection Law, Processor shall, to the extent reasonably practicable, inform Controller within a reasonable time, but such notice shall not create liability for Processor. Processor may refuse to execute instructions or to continue to process Data if it reasonably believes such instructions and/or processing are unlawful or violate Applicable Data Protection Laws, and shall promptly notify Controller of such refusal with reasons. For the avoidance of doubt, Processor shall neither sell the Data, as that term is used in the CCPA or permit access, disclose, or use the Data for its or another party's commercial purpose, except as set out in the Agreement and this DPA.

.

.

1.4. *Restricted transfers:* The parties agree that when the transfer of Data from Controller to Processor is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) in relation to Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will not apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be 14 (fourteen) days;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 13, the Irish Data Protection Commission shall act as competent supervisory authority;

(vi) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vii) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(viii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA;

(ix) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA; and

(x) Annex III of the EU SCCs shall be deemed completed with the information set out in Annex III to this DPA;

(b) in relation to Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

Controller and Processor will rely on the EU SCCs for transfers of personal data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:

(A) The EU SCCs, completed as set out above in clause 1.4(a) of this DPA shall also apply to transfers of such Data, subject to sub-clause (B) below;

(B) The UK Addendum shall be deemed executed between the transferring Controller and Processor, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Data.

In the event that any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. Processor may modify or amend the SCCs or addenda from time to time in order to comply with changing regulatory guidance, and without requiring re-execution of this DPA.

1.5. *Transfers:* Processor shall not participate in (nor permit any subprocessor to participate in) any other Restricted Transfers of Data unless the Restricted Transfer is made in full compliance with Applicable Data Protection Laws and subject to Controller's prior written instructions.

1.6. *Confidentiality of processing:* Processor shall ensure that any person that it authorises to process the Data (including Processor's staff, agents and subprocessors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a duty of confidentiality. Processor shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.

1.7. *Security:* Processor shall implement appropriate technical and organisational measures designed to protect the Data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access. Such measures shall be proportionate taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

At a minimum, such measures shall include the measures identified in Annex II.

1.8. *Subprocessing:* A list of approved subprocessors as at the date of this DPA is attached at Annex III, and Processor shall maintain and provide updated copies of this list to Controller upon request. Processor may from time to time engage other third party subprocessors to process the Data, provided that: (i) Processor provides at least 14 days' prior notice of the addition of any subprocessor (including details of the processing it performs or will perform); (ii) Processor imposes data protection obligations on any subprocessor it appoints that protect the Data, in substance, to the same standard provided for by this DPA; and (iii) Processor remains liable to Customer for the failure by any subprocessor to fulfil their data protection obligation. Failure of Controller to object within such 14-day period shall constitute consent.

1.9. *Cooperation and data subjects' rights:* Processor shall provide reasonable assistance to Controller by implementing appropriate technical and organizational measures, insofar as this is possible, taking into account the nature of the Processing, for the fulfilment of Controller's obligation to respond to data subjects' requests to exercise their rights, including their rights of access, correction, objection, erasure and data portability. Taking into account the nature of the Processing and the information available to the Processor, Processor will provide reasonable shall assistance to Controller in meeting its compliance obligations regarding: ensuring the security of the Data; and carrying out privacy and data protection impact assessments and related consultations of data protection authorities, Controller will pay Processor's for any such assistance, at Processor's then current fees.

1.10. *Security Incidents:* Processor shall notify Controller in writing without undue delay, and in any event within 72 hours of becoming aware of a confirmed Security Incident impacting the Controller directly. After providing notice, Processor shall investigate the Security Incident, take steps to eliminate or contain the exposure of the Data, and keep Controller informed of the status of the Security Incident. Processor further agrees to provide reasonable assistance and cooperation as requested by Controller in the furtherance of the correction or remediation of a Security Incident, and the mitigation of potential damage, including any legally required notification to be sent to affected individuals, regulators, or third parties. Taking into account the nature of Processing and the information available to Processor, Processor shall comply with, and shall assist Controller in complying with the obligations regarding Security Incident as set forth in Articles 33 and 34 of the GDPR.

1.11. *Deletion or Return of Data:* At Controller's discretion, Processor shall destroy or return all Data to Controller after the end of the provision of services relating to Processing and shall destroy existing copies unless applicable law requires storage of the Data. Notwithstanding the foregoing, Processor may retain backup copies for a commercially reasonable period for disaster recovery purposes, provided such Data remains subject to this DPA until securely deleted. If Processor has such a legal obligation to retain Data beyond the period otherwise specified by this clause 1.9, Processor shall notify Controller in writing of that obligation, to the extent permitted by applicable law, and shall return or destroy the Data in accordance with this clause 1.9 as soon as possible after that legally required retention period has ended.

1.12. *Limitation of Liability:* The total combined liability of either party and its affiliates towards the other party and its affiliates under or in connection with the Agreement and the DPA will be limited to and governed by the limitations set out in the Agreement.

1.13. *Audit:* Processor shall make available to Controller information reasonably necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including

inspections, conducted by the internal and external auditors and personnel of Controller and regulators, subject to each of the foregoing entering into a confidentiality agreement in a form acceptable to Processor in advance of such audit, at Controller's cost, limited to once per calendar year (unless required by law), at a time mutually agreed by the parties and with at least 90 days notice, and limited in scope to Processor's obligations under this DPA. In the event that Processor is found to be non-compliant with the terms of this DPA, Processor shall reimburse Controller for the direct costs and reasonable expenses of the audit. Notwithstanding the above, Processor will make available all current security compliance reports and certifications for the Controller to review before requiring any audit.

1.14. *Survival.* Processor's obligations under this DPA shall continue for so long as Processor continues to have access to, is in possession of, or acquires Data, even if the Agreement between Processor and Controller has expired or has been terminated.

Annex I

Data Processing Description

This Annex I forms part of the DPA and describes the processing that the processor will perform on behalf of the controller.

A. LIST OF PARTIES

Controller:

1. Name: *Customer*

Address: *Set out in Order Form*

Contact person's name, position and contact details: *Set out in Order Form*

Activities relevant to the data transferred under these Clauses: *Retail activities*

Signature and date: *As per the execution of the Order Form*

Role (controller/processor): *Controller*

Processor:

1. Name: *Tulip.io, Inc*

Address: *210-237 Glasgow Street, Office#192 Kitchener, ON N2G 4X8*

Contact person's name, position and contact details: *Set out in Order Form*

Activities relevant to the data transferred under these Clauses: *Provision of the Services consisting of the cloud-based delivery of one or more products specified in Order Forms.*

Signature and date: *Set out in Order Form*

Role (controller/processor): *Processor*

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Data subjects may be customers or prospective customers of Controller

Categories of personal data transferred:

Details of purchases of potential purchases

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Ongoing

Nature of the processing:

Access, storage, transfer in accordance with the terms of this DPA etc

Purpose(s) of the data transfer and further processing:

Provision of Services to Controller by Processor.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The Term of the MSA plus the period from the expiry of the MSA until the deletion of all Data by Processor in accordance with this DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

As specified in the link set out in Annex III.

Controller(s) / Data exporter(s): *Contact details ss laid out on the Order Form*

Annex II

Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Description of Measure	Tulip Actions and Controls
Measures of pseudonymisation and encryption of personal data	Tulip encrypts data in transit with TLS 1.2+ with chosen strong ciphers, at rest with AES-256. Tulip does not psuedoanonymise data in processing.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Tulip operates a formal information security program intended to provide confidentiality, integrity, availability and resilience of processing systems and services. Our program is built on policies, processes and procedures that are intended to provide that assurance. Tulip issues a SOC2 Type II audit report which details our program.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Tulip operates under redundant, re-createable systems that are hot-swappable and re-instantiable as needed to provide timely access to data. Databases are redundant across geographically dispersed datacentres, with backups in the cloud, appropriately encrypted and secured.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Tulip's internal processes include threat modeling proposed changes; review of all changes to systems; internal automated and manual security testing; externally sourced vulnerability scanning; and externally sourced penetration testing.
Measures for user identification and authorisation	The Tulip Platform leverages SAML for platform user permissions. For platform administration permissions, Tulip systems require strong password processes and two factor

	authentication. For internal Tulip identification and authorization, Tulip leverages Okta.
Measures for the protection of data during transmission	Data in transit is encrypted using TLS 1.2 or greater
Measures for the protection of data during storage	Data at rest is encrypted using AES 256.
Measures for ensuring physical security of locations at which personal data are processed	Tulip operates in Google Cloud Platform and has appropriate contracts with Google to ensure that their datacentres are appropriately secured. Tulip monitors and reviews Google's security reports, including its SOC2 Type II report.
Measures for ensuring events logging	Tulip has centralized logging through Google Stackdriver, storing logs for long-term storage in Google BigQuery and sending log events for analysis into our LogRhythm SIEM.
Measures for ensuring system configuration, including default configuration	Tulip operates via a Configuration as Code model, with no configuration manually performed. Tulip instead leverages Kubernetes/Docker container images for application code deployment and Terraform for managed service configuration. Kubernetes nodes are managed Google Kubernetes Environment infrastructure.
Measures for internal IT and IT security governance and management	Tulip operates a series of security measures. Please refer to the summary document attached. Please see our SOC2 Type II audit report for additional details.
Measures for certification/assurance of processes and products	Tulip issues a SOC2 Type II audit report yearly. Tulip also completes a PCI Attestation of Compliance, signed by an external Qualified Security Assessor.
Measures for ensuring data minimisation	Tulip depends on the data processing instructions of the client for data minimization. The client defines relevant fields within the application.

Measures for ensuring data quality	Tulip has functionality within its api and application to help with data quality, including import and synchronization functionality and a customizable customer capture/records entry form that can be tailored to a client's requirements.
Measures for ensuring limited data retention	Tulip has internal data retention policies. However, because Tulip synchronizes data with its clients, Tulip depends on those clients to initiate any data removal to comply with data retention policies in order to ensure that data corruption/accidental deletion does not occur.
Measures for ensuring accountability	Tulip considers both privacy and security as first class considerations within its work, including data processing; system design and system implementation. We have responsible parties within Tulip for both Security and Privacy.
Measures for allowing data portability and ensuring erasure	Tulip can provide, if needed, data exports. Tulip has processes and tools to ensure we can assist with Data Subject Requests. Tulip has configurable options for Data Subject Requests on removals, ensuring that data can be appropriately removed within the application. Should the contract with Tulip be terminated, Tulip removes client data via encryption key destruction, rendering both databases and database backups unreadable.

Annex III

Subprocessors

Controller has authorised the use of the sub-processors listed at https://tulip.com/subprocessors as updated from time to time.

Tulip has its subprocessors commit to the Standard Clauses, and only engages sub-processors with appropriate contracts.