Data Processing Addendum

This Data Processing Addendum ("DPA") supplements the Terms of Service (the "Agreement") between Turso Inc. ("Company," "us," "we") and the customer entity that is a party to the Agreement ("Customer" or "you"). We may update this Addendum from time to time, and we will provide reasonable notice of any such updates. Any terms not defined in this Addendum shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Customer's Personal Data to enable Company to perform its obligations under this DPA or the Agreement, and who is either (1) listed in Exhibit B or (2) subsequently authorized under Section 4.2 of this DPA.

1.3 "Company Account Data" means personal data that relates to Company's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Company Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.4 "Company Usage Data" means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.5 "Data Exporter" means Customer.

1.6 "Data Importer" means Company.

1.7 "Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including, without limitation: (i) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") (together, collectively, the "GDPR"), (iii) the Swiss Federal Act on Data Protection; (iv) the UK Data Protection Act 2018; and (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (vi) the Virginia Consumer Data Protection Act ("VCDPA"); (vii) the Colorado Privacy Act ("CPA"); (viii) the Connecticut Data Privacy Act ("CTDPA"), and (ix) the Utah Consumer Privacy Act ("UCPA"); (x) the Personal Information Protection and Electronic Documents Act (Canada) ("PIPEDA"); (xi) An Act respecting the protection of personal information in the private sector (Québec), as amended by Law 25 (the "Quebec Privacy Act"); (xii) the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados, Law No. 13,709/2018) ("LGPD"); and (xiii) any other applicable data protection, privacy, or data security laws and regulations of any relevant jurisdiction; in each case, as updated, amended or replaced from time to time. The terms "Data Subject", "Personal Data", "Personal Data Breach", "processing", "processor," "controller," and "supervisory authority" shall have the meanings set forth in the GDPR.

1.1 "Data Privacy Framework" means, as applicable, EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S. Data Privacy Framework.

1.8 "EU SCCs" means, as applicable, the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 6.2 of this DPA.

1.9 "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.10 "ex-UK Transfer" means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is

processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the "UK"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.11"Services" shall have the meaning set forth in the Agreement.

1.12 "Standard Contractual Clauses" means the EU SCCs and the UK SCCs.

1.13"UK Addendum" has the meaning set forth in Exhibit D.

1.14"UK SCCs" means the EU SCCs, as amended by the UK Addendum.

2. Relationship of the Parties; Processing of Data

2.1 The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this DPA or the Agreement, Company is a processor. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith.

2.2 Company shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Company is subject; in such a case, the Company shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Customer hereby instructs Company to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

1.2 The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.

2.3 Following completion of the Services, at Customer's choice, Company shall return or delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Company to Customer only upon Customer's request.

1.3 State Privacy Law Language. The Parties acknowledge and agree that the processing of personal information or personal data that is subject to the CCPA, VCDPA, CPA, CTDPA, or UCPA shall be carried out in accordance with the terms set forth in Exhibit E.

1.4 International Privacy Law Language. The Parties acknowledge and agree that the processing of personal information or personal data that is subject to PIPEDA, the Quebec Privacy Act, or the LGPD shall be carried out in accordance with the terms set forth in Exhibit F.

3. Confidentiality

Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

4. Authorized Sub-Processors

4.1 Customer acknowledges and agrees that Company may (1) engage its Affiliates and the Authorized Sub-Processors listed in Exhibit B to this DPA to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without

limitation the processing of Personal Data. By way of this DPA, Customer provides general written authorization to Company to engage sub-processors as necessary to perform the Services.

4.2 A list of Company's current Authorized Sub-Processors (the "List") will be made available to Customer, either at https://trust.turso.tech, via email or through another means made available to Customer. Such List may be updated by Company from time to time. Company may provide a mechanism to subscribe to notifications of new Authorized Sub-Processors and Customer agrees to subscribe to such notifications where available. At least ten (10) days before enabling any third party other than existing Authorized Sub-Processors to access or participate in the processing of Personal Data, Company will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing Company within ten (10) days of receipt of the aforementioned notice by Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Company from offering the Services to Customer.

4.3 If Customer reasonably objects to an engagement in accordance with Section 4.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Company. Discontinuation shall not relieve Customer of any fees owed to Company under the Agreement.

4.4 If Customer does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Company, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.

4.5 Company will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Company under this DPA with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations under such agreement.

4.6 If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Company to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Company beforehand, and that such copies will be provided by the Company only upon request by Customer.

5. Security of Personal Data.

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, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit C sets forth additional information about Company's technical and organizational security measures.

2. Transfers of Personal Data

5.1 The parties agree that Company may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations take place in the United States, and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. If Company transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

5.2 Ex-EEA Transfers. The parties agree that ex-EEA Transfers will be made (i) pursuant to the Data Privacy Framework, or (ii) if the Data Privacy Framework does not apply, pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

5.2.1 Module One (Controller to Controller) of the EU SCCs apply when Company is processing Personal Data as a controller pursuant to Section 9 of this DPA.

5.2.2 Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Company is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA.

5.2.3 Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor

and Company is processing Personal Data on behalf of Customer as a sub-processor.

5.3 For each module, where applicable the following applies:

5.3.1 The optional docking clause in Clause 7 does not apply;

5.3.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4.2 of this DPA;

5.3.3 In Clause 11, the optional language does not apply;

5.3.4 All square brackets in Clause 13 are hereby removed;

5.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by the laws of the Republic of Ireland; **5.3.6** In Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland;

5.3.7 Exhibit B to this DPA contains the information required in Annex I and Annex III of the EU SCCs;

5.3.8 Exhibit C to this DPA contains the information required in Annex II of the EU SCCs; and

5.3.9 By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

5.4 Ex-UK Transfers. The parties agree that ex-UK Transfers will be made (i) pursuant to the Data Privacy Framework, or (ii) if the Data Privacy Framework does not apply, pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed in accordance with the UK Addendum, which is incorporated herein as Exhibit D of this DPA.

5.5 Transfers from Switzerland. The parties agree that transfers from Switzerland will be made (i) pursuant to the Data Privacy Framework, or (ii) if the Data Privacy Framework does not apply, pursuant to the EU SCCs with the following modifications:

5.5.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

5.5.2 The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

5.5.3 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.

5.5.4 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

5.6 Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer made pursuant to the Standard Contractual Clauses, the following supplementary measures shall apply:

5.6.1 As of the date of this DPA, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer's Personal Data ("Government Agency Requests");

5.6.2 If, after the date of this DPA, the Data Importer receives any Government Agency Requests, Company shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If compelled to disclose Customer's Personal Data to a law enforcement or government agency, Company shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of the such

Government Agency Requests;

5.6.3 The Data Exporter and Data Importer will meet regularly to consider whether:

(i) the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

(ii) additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

(iii) it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

5.6.4 If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

5.6.5 If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

3. Rights of Data Subjects

5.7 Company shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Company receives a Data Subject Request in relation to Customer's data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

5.8 Company shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

6. Actions and Access Requests; Audits

3.1 Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, *provided that* Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

3.2 Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

6.1 Company shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA, and retain such records for a period of three (3) years after the termination of the Agreement. Customer

shall, with reasonable notice to Company, have the right to review, audit and copy such records at Company's offices during regular business hours.

6.2 Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under Data Protection Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 8.4.

6.3 Company shall immediately notify Customer if an instruction, in the Company's opinion, infringes the Data Protection Laws or Supervisory Authority.

6.4 In the event of a Personal Data Breach, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Company's reasonable control).

6.5 In the event of a Personal Data Breach, Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

6.6 The obligations described in Sections 8.6 and 8.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 8.6 and 8.7 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

7. Company's Role as a Controller. The parties acknowledge and agree that with respect to Company Account Data and Company Usage Data, Company is an independent controller, not a joint controller with Customer. Company will process Company Account Data and Company Usage Data as a controller (i) to manage the relationship with Customer; (ii) to carry out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement. Company may also process Company Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by the Company as a controller shall be in accordance with the Company's privacy policy set forth at https://turso.tech/privacy-policy.

8. **Conflict.** In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement; and (4) the Company's privacy policy. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

11. Execution of this DPA. Company has pre-signed this DPA in the signature block below and in Exhibit B (as the "data importer"). To complete this DPA, Customer must: (i) complete the information requested in the signature block below and sign there. Upon receipt of the validly completed Addendum by Company at this email address, this DPA will become legally binding. For the avoidance of doubt, signature of the DPA shall be deemed to constitute signature and acceptance of the EU SCCs incorporated herein, including their appendices.

Customer:	**Turso Inc.**
Signature	Signature
Print Name	Print Name
Title	Title
Date	Date

Exhibit A

Details of Processing

Nature and Purpose of Processing: Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes, without limitation:

Receiving data, including collection, accessing, retrieval, recording, and data entry
Holding data, including storage, organization and structuring
Using data, including analysis, consultation, testing, automated decision making and profiling
Updating data, including correcting, adaptation, alteration, alignment and combination
Protecting data, including restricting, encrypting, and security testing
Sharing data, including disclosure, dissemination, allowing access or otherwise making available Returning data to the data exporter or data subject
Erasing data, including destruction and deletion

Duration of Processing: Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable

law or regulation. Company Account Data and Company Usage Data will be processed and stored as set forth in Company's privacy policy.

Categories of Data Subjects: The categories of Data Subject to which Customer's Personal Data will relate are determined and controlled by the Customer in its sole discretion and may include, but are not limited to, Customer end-users and customers and Customer personnel.

Categories of Personal Data: Company processes Personal Data contained in Company Account Data, Company Usage Data, and any Personal Data provided by Customer (including any Personal Data Customer collects from its end users and processes through its use of the Services) or collected by Company in order to provide the Services or as otherwise set forth in the Agreement or this DPA. Categories of Personal Data are determined and controlled by the Customer in its sole discretion and may include, but are not limited to, name, location, email address, phone number, address, occupation, and title.

Sensitive Data or Special Categories of Data: None to the knowledge of the Company.

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. The Parties

Data exporter(s): The Customer

Contact details: As designated by Customer in Customer's account.

Signature and date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

Role (controller/processor): The Data Exporter's role is set forth in Section 2 of this Addendum.

Data importer(s): Turso Inc.

Address: 2093 Philadelphia Pike, #6336 Claymont, Delaware 19703 United States

Contact person's name, position and contact details: Glauber Costa, CEO, glauber@turso.tech

Signature and date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses

incorporated herein, as of the Effective Date of the Agreement.

Role (controller/processor): The Data Importer's role is set forth in Section 2 of this Addendum.

2. Description of the Transfer

Data Subjects	As described in Exhibit A of the DPA.
Categories of Personal Data	As described in Exhibit A of the DPA.
Special Category Personal Data (if applicable)	As described in Exhibit A of the DPA.
Nature of the Processing	As described in Exhibit A of the DPA.
Purposes of Processing	As described in Exhibit A of the DPA.
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the DPA.
Frequency of the transfer	As necessary to provide and perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA.
Recipients of Personal Data Transferred to the Data Importer	Company's list of Subprocessors can be found at: https://trust.turso.tech

3. Competent Supervisory Authority
The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

4. List of Authorized Sub-Processors
The Company shall maintain an up-to-date list of Sub-Processors at the following URL: https://trust.turso.tech

Exhibit C

Description of the Technical and Organisational Security Measures implemented by the Data Importer

To view a summary of the technical and organisational security measure the Company has in place to protect personal data, please visit the following URL: https://trust.turso.tech

Exhibit D

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Customer	Company
Key Contact	*See* Exhibit B of this DPA	*See* Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Section 6.2 and 6.3 of the DPA.

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: Description of Transfer	*See* Exhibit B of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	*See* Exhibit C of this DPA
Annex III: List of Sub processors (Modules 2 and 3 only):	*See* Exhibit B of this DPA

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	☒ Importer ☒ Exporter ☐ Neither Party

Entering into this UK Addendum:

1. Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the

same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

UK Addendum	means this International Data Transfer Addendum incorporating the EU SCCs, attached to the DPA as Exhibit D.

EU SCCs	means the version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information
Appendix Information	shall be as set out in Table 3
Appropriate Safeguards	means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making an ex-UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	means the template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under Section 18 of the UK Addendum.
Approved EU SCCs	means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).
ICO	means the Information Commissioner of the United Kingdom.
ex-UK Transfer	shall have the same definition as set forth in the DPA .
UK	means the United Kingdom of Great Britain and Northern Ireland
UK Data Protection Laws	means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	shall have the definition set forth in the DPA.

4. The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws applies.

7. If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for ex-UK Transfers, the hierarchy in Section 10 below will prevail.

10. Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.

11. Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

Incorporation and Changes to the EU SCCs:

12. This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:

a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b) Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and

c) the UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales.

13. Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.

15. The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made:

a) References to the "Clauses" means this UK Addendum, incorporating the EU SCCs;

b) In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679",

c) Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d) Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e) Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g) References to Regulation (EU) 2018/1725 are removed;

h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j) Clause 13(a) and Part C of Annex I are not used;

k) The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l) In Clause 16(e), subsection (i) is replaced with: “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m) Clause 17 is replaced with: “These Clauses are governed by the laws of England and Wales”

n) Clause 18 is replaced with: “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales.” A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts.”; and

o) The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to the UK Addendum

16. The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland and Northern Ireland.

17. If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved UK Addendum which:

a) makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

b) reflects changes to UK Data Protection Laws;

The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

19. If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

c) its direct costs of performing its obligations under the UK Addendum; and/or

d) its risk under the UK Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

20. The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

Exhibit E

United States Privacy Law Exhibit

This United States Privacy Law Exhibit ("Exhibit") supplements the DPA and includes additional information required by the CCPA, the VCDPA, the CPA, the CTDPA, and the UCPA in each case, as updated, amended or replaced from time to time. Any terms not defined in this Exhibit shall have the meanings set forth in the DPA and/or the Agreement.

A. CALIFORNIA

1. Definitions

1.1 For purposes of this Section A, the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" shall have the meanings set forth in the CCPA.

1.2 All references to "Personal Data," "Controller," "Processor," and "Data Subject" in the DPA shall be deemed to be references to "Personal Information," "Business," "Service Provider," and "Consumer," respectively, as defined in the CCPA.

2. Obligations

2.1 Except with respect to Company Account Data and Company Usage Data (as defined in the DPA), the parties acknowledge and agree that Company is a Service Provider for the purposes of the CCPA (to the extent it applies) and Company is receiving Personal Information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.

2.2 Customer shall disclose Personal Information to Company only for the limited and specified purposes described in Exhibit A to this DPA.

2.3 Company shall not Sell or Share Personal Information provided by Customer under the Agreement.

2.4 Company shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the CCPA.

2.5 Company shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement outside of the direct business relationship between Company and Customer, except where and to the extent permitted by the CCPA.

2.6 Company shall notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA.

2.7 Company will not combine Personal Information received from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

2.8 Company shall comply with all obligations applicable to Service Providers under the CCPA, including by providing Personal Information provided by Customer under the Agreement the level of privacy protection required by CCPA.

2.9 Company shall only engage a new sub-processor to assist Company in providing the Services to Customer under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4.1 of the DPA at least ten (10) days before enabling a new Sub-Processor; and (ii) entering into a written contract with the sub-processor requiring sub-processor to observe all of the applicable requirements set forth in the CCPA.

3. Consumer Rights

3.1 Company shall assist Customer in responding to Verifiable Consumer Requests to exercise the Consumer's rights under the CCPA as set forth in Section 7 of the DPA.

4. Audit and Remediation Rights

4.1 To the extent required by CCPA, Company shall allow Customer to conduct inspections or audits in accordance with Sections 8.3 and 8.4 of the DPA.

4.2 If Customer determines that Company is Processing Personal Information in an unauthorized manner, Customer may, taking into account the nature of the Company's Processing and the nature of the Personal Information Processed by Company on behalf of Customer, take commercially reasonable and appropriate steps to stop and remediate such unauthorized Processing.

B. VIRGINIA

1. Definitions

1.1 For purposes of this Section B, the terms "Consumer," "Controller," "Personal Data," "Processing," and "Processor" shall have the meanings set forth in the VCDPA.

1.2 All references to "Data Subject" in this DPA shall be deemed to be references to "Consumer" as defined in the VCDPA.

2. Obligations

2.1 Except with respect to Company Account Data and Company Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Company is a Processor for the purposes of the VCDPA (to extent it applies).

2.2 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.3 Company shall adhere to Customer's instructions with respect to the Processing of Customer Personal Data and shall assist Customer in meeting its obligations under the VCDPA by:

2.3.1 Assisting Customer in responding to Consumer rights requests under the VCDPA as set forth in Section 7 of the DPA;

2.3.2 Complying with Section 5 ("Security of Personal Data") of the DPA with respect to Personal Data provided by Customer;

2.3.3 In the event of a Personal Data Breach, providing information sufficient to enable Customer to meet its obligations pursuant to Va. Code § 18.2-186.6; and

2.3.4 Providing information sufficient to enable Customer to conduct and document data protection assessments to the extent required by VCDPA.

2.4 Company shall maintain the confidentiality of Personal Data provided by Customer and require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;

2.5 Upon Customer's written request, Company shall delete or return all Personal Data provided by Customer in accordance with Section 2.4 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

2.6 In the event that Company engages a new sub-processor to assist Company in providing the Services to Customer under the Agreement, Company shall enter into a written contract with the sub-processor requiring sub-processor to observe all of the applicable requirements of a Processor set forth in the VCDPA.

3. **Audit Rights**

3.1 Upon Customer's written request at reasonable intervals, Company shall, as set forth in Sections 8.3-8.4 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Company's compliance with its obligations under the VCDPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the VCDPA.

COLORADO

1. Definitions

1.1 For purposes of this Section C, the terms "Consumer," "Controller," "Personal Data," "Processing," and "Processor" shall have the meanings set forth in the CPA.

1.2 All references to "Data Subject" in the DPA shall be deemed to be references to "Consumer" as defined in the CPA.

2. Obligations

3.2 Except with respect to Company Account Data and Company Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Company is a Processor for the purposes of the CPA (to extent it applies).

3.3 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

3.4 Company shall require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing.

3.5 Company shall only engage a new subcontractor to assist Company in providing the Services to Customer under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4.1 of the DPA and providing Customer with an opportunity to object and (ii) entering into a written contract with the subcontractor requiring subcontractor to observe all of the applicable requirements set forth in the CPA.

3.6 Company shall be responsible for taking the appropriate technical and organizational measures as described in Exhibit C. Customer shall be responsible for implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

3.7 Upon Customer's written request, Company shall delete or return all Personal Data provided by Customer in accordance with Section 2.4 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

4. Audit Rights

4.1 Upon Customer's written request at reasonable intervals, Company shall, as set forth in Sections 8.3-8.4 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Company's compliance with its obligations under the CPA and (ii) allow and cooperate with reasonable inspections or audits as required or permitted under the CPA.

D. CONNECTICUT

1. Definitions

1.1 For purposes of this Section D, the terms "Consumer," "Controller," "Personal Data," "Processing," and "Processor" shall have the meanings set forth in the CTDPA.

1.2 All references to "Data Subject" in the DPA shall be deemed to be references to "Consumer" as defined in the CTDPA.

2. Obligations

4.2 Except with respect to Company Account Data and Company Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Company is a Processor for the purposes of the CTDPA (to extent it applies).

4.3 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

4.4 Company shall require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing.

4.5 Company shall only engage a new subcontractor to assist Company in providing the Services to Customer under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4.1 of the DPA and providing Customer with an opportunity to object and (ii) entering into a written contract with the subcontractor requiring subcontractor to observe all of the applicable requirements set forth in the CTDPA.

4.6 Upon Customer's written request, Company shall delete or return all Personal Data provided by Customer in accordance with Section 2.4 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

5. Audit Rights

5.1 Upon Customer's written request at reasonable intervals, Company shall, as set forth in Sections 8.3-8.4 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Company's compliance with its obligations under the CTDPA and (ii) allow and cooperate with reasonable inspections or audits as required under the CTDPA.

E. UTAH

1. Definitions

1.1 For purposes of this Section E, the terms "Consumer," "Controller," "Personal Data," "Processing," and "Processor" shall have the meanings set forth in the UCPA.

1.2 All references to "Data Subject" in the DPA shall be deemed to be references to "Consumer" as defined in the UCPA.

2. Obligations

5.2 Except with respect to Company Account Data and Company Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Company is a Processor for the purposes of the UCPA (to extent it applies).

5.3 The instructions with respect to the Processing of Customer Personal Data and the parties' rights and obligations are set forth in this DPA and the Agreement.

5.4 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

5.5 Company shall require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing.

5.6 Company shall only engage a new subcontractor to assist Company in providing the Services to Customer under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by entering into a written contract with the subcontractor requiring subcontractor to observe all of the applicable requirements set forth in the UCPA.

Exhibit F

International Data Protection Laws Exhibit

This International Data Protection Laws Exhibit ("Exhibit") supplements the DPA and includes additional terms required by the data protection laws of Canada (including the Province of Québec) and Brazil, in each case as updated, amended or replaced from time to time. Any terms not defined in this Exhibit shall have the meanings set forth in the DPA and/or the Agreement. This Exhibit applies only to the extent that the processing of Personal Data by Company on behalf of Customer is subject to the applicable law identified in the relevant Section below. In the event of a conflict between this Exhibit and the other provisions of the DPA with respect to such processing, this Exhibit shall control.

A. CANADA

1. Definitions

1.1 For purposes of this Section A, "PIPEDA" means the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), as amended; "Quebec Privacy Act" means An Act respecting the protection of personal information in the private sector (CQLR, c. P-39.1), as amended by the Act to modernize legislative provisions as regards the protection of personal information ("Law 25"); and "Canadian Privacy Laws" means PIPEDA and the Quebec Privacy Act, collectively. The terms "personal information," "organization," and "commercial activity" shall have the meanings set forth in the applicable Canadian Privacy Laws.

1.2 To the extent the Canadian Privacy Laws apply, all references to "Personal Data" and "Data Subject" in the DPA shall be deemed to be references to "personal information" and to the individual to whom such personal information relates, respectively, as those concepts are used in the Canadian Privacy Laws.

2. Obligations

2.1 Except with respect to Company Account Data and Company Usage Data (as defined in the DPA), the parties acknowledge and agree that, to the extent the Canadian Privacy Laws apply, Customer is the organization accountable for the personal information it entrusts to Company, and Company processes such personal information solely as a service provider and mandatary on behalf of, and for the purposes determined by, Customer.

2.2 Company shall use and process personal information provided by Customer only to the extent necessary to provide the Services under the Agreement and in accordance with Customer's documented instructions, and shall not retain, use, communicate, or otherwise process such personal information for any other purpose.

2.3 Company shall ensure that each person it authorizes to process such personal information is subject to an obligation of confidentiality and processes the personal information only as necessary to perform the Services.

2.4 Company shall implement and maintain technical and organizational security measures appropriate to the sensitivity of the personal information, as further described in Exhibit C, to protect the personal information against loss and against unauthorized access, disclosure, copying, use, or modification.

2.5 Company shall not retain personal information provided by Customer for longer than necessary to fulfil its obligations under the Agreement and this DPA and, upon completion of the Services, shall return or destroy such personal information in accordance with Section 2.4 of the DPA, unless retention is required or authorized by applicable law.

2.6 Company shall engage sub-processors only in accordance with Section 4 of the DPA and shall enter into a written contract with each sub-processor imposing obligations for the protection of personal information that are substantially similar to, and no less protective than, those imposed on Company under this DPA and required by the Canadian Privacy Laws.

2.7 In the event of a confidentiality incident (within the meaning of the Quebec Privacy Act) or a breach of security safeguards (within the meaning of PIPEDA) involving personal information provided by Customer, Company shall notify Customer without undue delay in accordance with Sections 8.6–8.7 of the DPA and provide Customer with reasonable cooperation and information to enable Customer to assess the risk of injury and to comply with its own notification and record-keeping obligations under the Canadian Privacy Laws.

2.8 Taking into account the nature of the processing, Company shall provide Customer with reasonable assistance necessary for Customer to (i) conduct any privacy impact assessment required under the Quebec Privacy Act, including in connection with the communication of personal information outside Québec, and (ii) respond to inquiries, requests, or investigations from the Commission d'accès à l'information du Québec or the Office of the Privacy Commissioner of Canada.

3. Communication of Personal Information Outside Québec and Canada

3.1 Customer acknowledges that Company's primary processing operations take place in the United States, and that

the provision of the Services involves the communication of personal information outside the Province of Québec and outside Canada. Upon Customer's reasonable request, Company shall provide information regarding the safeguards it has implemented (including those described in Exhibit C) to assist Customer in conducting any privacy impact assessment required prior to such communication and in assessing whether the personal information would receive protection that is adequate in light of generally recognized principles of data protection.

4. Individual Rights

4.1 Company shall, in accordance with Section 7 of the DPA, provide Customer with reasonable assistance to enable Customer to respond to requests from individuals seeking to exercise their rights under the Canadian Privacy Laws, including rights of access, rectification, withdrawal of consent, de-indexing, and portability, in each case to the extent applicable.

5. Audit Rights

5.1 Upon Customer's written request at reasonable intervals, Company shall, as set forth in Sections 8.3–8.4 of the DPA, (i) make available to Customer information reasonably necessary to demonstrate Company's compliance with its obligations under the Canadian Privacy Laws, and (ii) allow and cooperate with reasonable inspections or audits, including verification of the safeguards implemented by Company.

B. BRAZIL

1. Definitions

1.1 For purposes of this Section B, "LGPD" means the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, Law No. 13,709/2018), as amended; and "ANPD" means the Brazilian National Data Protection Authority (Autoridade Nacional de Proteção de Dados). The terms "controller," "operator," "processing agent," "data subject," "personal data," and "processing" shall have the meanings set forth in the LGPD.

1.2 To the extent the LGPD applies, all references to "Processor" in the DPA shall be deemed to be references to "operator" (operador), and all references to "Data Subject" shall be deemed to be references to "data subject" (titular), as defined in the LGPD.

2. Obligations

2.1 Except with respect to Company Account Data and Company Usage Data (as defined in the DPA), the parties acknowledge and agree that, to the extent the LGPD applies, Customer acts as controller and Company acts as operator, processing personal data on behalf of Customer and pursuant to Customer's documented instructions.

2.2 Company shall process personal data only in accordance with Customer's lawful, documented instructions and the Agreement, and shall not process such personal data for its own purposes. If Company is of the opinion that an instruction infringes the LGPD, Company shall promptly notify Customer.

2.3 Company shall ensure that each person it authorizes to process the personal data is bound by an obligation of confidentiality.

2.4 Company shall adopt security, technical, and administrative measures able to protect the personal data from unauthorized access and from accidental or unlawful destruction, loss, alteration, communication, or dissemination, as further described in Exhibit C and consistent with Articles 46 to 49 of the LGPD.

2.5 In the event of a security incident that may create relevant risk or harm to data subjects, Company shall notify Customer without undue delay in accordance with Sections 8.6–8.7 of the DPA and provide the information reasonably necessary to enable Customer, as controller, to communicate the incident to the ANPD and to affected data subjects within the timeframe and in the manner required by the LGPD and applicable ANPD regulations.

2.6 Company shall engage sub-processors (sub-operators) only in accordance with Section 4 of the DPA and shall impose on each such sub-operator, by written contract, data protection obligations that are substantially similar to, and no less protective than, those set out in this DPA and required by the LGPD. Company shall remain liable to Customer for the acts and omissions of its sub-operators.

2.7 Taking into account the nature of the processing, Company shall provide Customer with reasonable assistance to enable Customer to comply with its obligations under the LGPD, including in responding to data subject requests, in preparing any report of impact to the protection of personal data (relatório de impacto à proteção de dados pessoais), and in responding to requests or determinations of the ANPD.

2.8 Company shall maintain records of the processing operations it carries out on behalf of Customer, as contemplated by Article 37 of the LGPD.

2.9 Upon termination of the processing, Company shall eliminate the personal data in accordance with Section 2.4 of

the DPA and Article 15 of the LGPD, except where retention is authorized by the LGPD.

3. International Data Transfers

3.1 Customer acknowledges that Company's primary processing operations take place in the United States, and that the provision of the Services involves the transfer of personal data outside Brazil to the United States. Section 3.2 applies to any such transfer that constitutes an international data transfer subject to the LGPD.

3.2 To the extent a transfer of personal data outside Brazil under this DPA constitutes an international data transfer subject to the LGPD that is not covered by an adequacy decision of the ANPD or another lawful basis for international data transfer under Article 33 of the LGPD, the parties shall, upon Customer's request, enter into the standard contractual clauses approved by the ANPD in Resolution CD/ANPD No. 19/2024 (the "ANPD SCCs"), or put in place another transfer mechanism permitted under Article 33 of the LGPD. Company shall provide reasonable cooperation to give effect to such mechanism. The parties acknowledge that the ANPD SCCs are a prescribed form that may not be modified by the parties.

4. Data Subject Rights

4.1 Company shall, in accordance with Section 7 of the DPA, provide Customer with reasonable assistance to enable Customer to respond to requests from data subjects seeking to exercise their rights under Article 18 of the LGPD, including confirmation of the existence of processing, access, correction, anonymization, blocking or elimination, portability, information about sharing, and revocation of consent.

5. Audit Rights

5.1 Upon Customer's written request at reasonable intervals, Company shall, as set forth in Sections 8.3–8.4 of the DPA, (i) make available to Customer information reasonably necessary to demonstrate its compliance with its obligations as operator under the LGPD, and (ii) allow and cooperate with reasonable inspections or audits.