DBT LABS
DATA PROCESSING ADDENDUM

1. BACKGROUND

1.1. This Data Processing Addendum, including the terms and conditions sets out in the Schedules attached hereto (collectively, "**DPA**"), is an addendum to the signed underlying master agreement between the parties (the "**Agreement**"), and is entered between dbt Labs, Inc., a Delaware corporation with its principal place of business at 915 Spring Garden St., Suite 500, Philadelphia, PA 19123 USA ("**dbt Labs**"), and **Subscriber**.

1.2. This DPA applies where and only to the extent that dbt Labs Processes Subscriber Personal Data (each as defined below) on behalf of Subscriber as a Processor (as defined below) in the course of providing the Services (as defined in the Agreement), and: (i) such Subscriber Personal Data relates to Data Subjects located in the EEA, United Kingdom ("**UK**"), or Switzerland, (ii) Subscriber is a Business or a Controller, and/or (iii) the applicable obligations as described herein are required under Data Protection Laws. This DPA only applies in a jurisdiction to the extent such obligations are required by applicable law in that jurisdiction, and the law of one jurisdiction will not apply outside that jurisdiction to the maximum extent permitted by applicable law. The parties agree to comply with the Data Protection Laws applicable to their respective roles of using the Service for Subscriber and providing Services for dbt Labs.

1.3. This DPA will replace any previously applicable data processing addendum as from the DPA Effective Date (as defined below). In the event of a conflict between any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail as to matters of privacy and data protection.

2. DEFINITIONS. Unless otherwise set out below, each capitalised term in this DPA shall have the meaning set out in the Agreement, and the following capitalised terms used in this DPA shall be defined as follows:

2.1. "Controller to Processor Clauses" means (i) in respect of transfers of Personal Data from the European Economic Area ("EEA"), Module 2 (Controller to Processor) of the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021; (ii) in respect of transfers of Personal Data from the UK, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, in force 21 March 2022" to the SCCs, with Subscriber as data exporter and dbt Labs as data importer, or any equivalent clauses issued by the relevant competent

authority of the UK ("**UK Addendum**"), and (iii) in respect of transfers of Personal Data from the Switzerland, a version of the applicable clauses referenced at (i) above that includes all necessary amendments to make them legally effective in Switzerland, including but not limited to the following: references to the GDPR will be deemed to be references to the Swiss privacy laws including the Federal Act on Data Protection ("**FADP**"), references to "Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with Clause 18(c) , in each case as amended and replaced from time to time.

2.2. **"Data Protection Laws"** means all laws and regulations applicable to the processing of Personal Data by dbt Labs in its provision of Services to Subscriber, including (i) the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council (**"GDPR"**); (ii) the Privacy and Electronic Communications Directive 2002/58/EC; (iii) the UK Data Protection Act 2018, the UK General Data Protection Regulation as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and the Privacy and Electronic Communications Regulations 2003; (iv) the FADP; (v) the California Consumer Privacy Act of 2018 (**"CCPA"**) as updated by the California Privacy Rights Act of 2020 ("**CPRA**"), including any regulations promulgated thereunder, as amended from time to time; and (vi) once enforced, the applicable laws and regulations enacted by and in effect in any other U.S. states and/or the U.S. Federal government, as amended or replaced from time to time, including but not limited to Illinois, Virginia, Colorado, Texas, and Utah; and (vii) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of Personal Data; and applicable to each of the foregoing subsections, as such acts and regulations are in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

2.3. **"DPA Effective Date"** means the date on which Subscriber accepted, or the parties otherwise agreed to, this DPA.

2.4. **"European Economic Area"** or **"EEA"** means the Member States of the European Union together with Iceland, Norway, and Liechtenstein.

2.5. **"Personal Data"** shall mean any Subscriber personal information or similar term (as defined by applicable Data Protection Laws) that is subject to the Data Protection Laws.

2.6. "**Processor to Processor Clauses**" means as relevant, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021 specifically including Module 3 (Processor to Processor), or any equivalent clauses issued by the relevant competent authorities of the UK, in respect of transfers of Personal Data from the UK, and the FADP, in respect of transfers of Personal Data from Switzerland, in each case as in force and as amended, updated or replaced from time to time.

2.7. **"Regulator"** means a data protection or privacy regulator or supervisory authority which has jurisdiction over a Controller's Processing of Personal Data.

2.8. **"Security Incident"** means a breach of dbt Labs's security leading to the accidental or unlawful destruction, loss, alteration, disclosure of, or access to, any Subscriber Personal Data while in the possession and control of dbt Labs.

2.9. **"Standard Contractual Clauses" or "SCCs"** means both the: (i) Controller to Processor Clauses; and (ii) Processor to Processor Clauses (as applicable).

2.10. **"Subprocessor"** means any Processor engaged directly by dbt Labs who agrees to Process Subscriber Personal Data on behalf of dbt Labs and is providing the principal services. This excludes ancillary services, such as telecommunication or internet connection services, maintenance, training or user support services, or measures that support the operation of, or ensure the confidentiality, availability, integrity and resilience of, hardware and software. dbt Labs will, however, make appropriate and legally binding contractual arrangements with such ancillary services including requirements to protect Client Data and inspection measures to confirm compliance.

2.11. **"Subscriber Personal Data"** means Personal Data, that dbt Labs Processes on behalf of the Subscriber in connection with dbt Labs's provision of the Service.

2.12. **"Third Country"** means (i) in relation to Personal Data transfers from the EEA, any country outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time to the extent dbt Labs has complied with the adequacy ruling obligations having such ruling of adequate protection; and (ii) in relation to Personal Data transfers from the UK, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing

adequate protection for Personal Data by the relevant competent authority of the UK from time to time.

2.13. The terms **"Controller", “Data Subject”, "Processor", and "Process"** shall have the same meaning as set out in the GDPR, irrespective of whether European or non-European Data Protection Laws apply.

2.14. The terms **"Business", "Service Provider", “Share” and “Sell”** (and their conjugates) shall have the same meaning as set out in the CCPA/CPRA.

3. DATA PROCESSING

3.1. Instructions for Data Processing. dbt Labs will only Process Subscriber Personal Data as a Processor or Service Provider, as applicable, in accordance with the Agreement and pursuant to the processing details set out in Schedule 1, to the extent necessary to provide the Service to the Subscriber, and the Subscriber's written instructions provided to dbt Labs (the **"Permitted Purpose"**), unless Processing is otherwise required or permitted by the Data Protection Laws to which dbt Labs is subject, in which case dbt Labs shall, to the extent required or permitted by such Data Protection Laws, inform the Subscriber of that legal requirement before Processing that Subscriber Personal Data. dbt Labs shall not Sell, Share, retain, use, disclose or Process Subscriber Personal Data, or combine the Subscriber Personal Data received from or on behalf of the business with personal information dbt Labs received elsewhere, unless specific statutory or regulatory exceptions apply (i) for any purposes other than the Permitted Purpose, or (ii) outside of the direct business relationship between dbt Labs and Subscriber. Should dbt Labs no longer be able to comply with this subsection, dbt Labs will cease processing Subscriber Personal Data and notify Subscriber, and Subscriber may take reasonable and appropriate steps to (a) determine dbt Labs’s compliance herewith, subject to Section 5.3 hereof; and/or (b) may terminate the Agreement, to be effective upon payment in full of Fees, and request in writing for dbt Labs to delete without undue delay Subscriber Personal Data after receiving notice that dbt Labs can no longer meet its CPRA obligations.

3.2. The Agreement and this DPA shall be the Subscriber's complete and final instructions to dbt Labs in relation to the processing of Subscriber Personal Data. In the event dbt Labs reasonably believes that the Subscriber’s written instructions violate applicable law, dbt Labs will inform the Subscriber in writing, and not be required to fulfill any such instructions.

3.3. Processing outside the scope of this DPA will require a prior written agreement between the Subscriber and dbt Labs.

3.4. Required consents. The Subscriber represents and warrants that it has sent all applicable notices to Data Subjects consistent with and required under applicable Data Protection Laws to permit the lawful Processing of Subscriber Personal Data by dbt Labs in accordance with the Agreement. Where required by applicable Data Protection Laws, Subscriber warrants that it will ensure that it has obtained/will obtain all necessary consents, permissions, authorizations, and approvals to the extent required by Data Protection Laws for the lawful Processing of Subscriber Personal Data by dbt Labs in accordance with the Agreement.

3.5. Subscriber warrants it lawfully discloses and has a legitimate ground to disclose Subscriber Personal Data to dbt Labs and enable the Processing of the Personal Data by dbt Labs as set out in this DPA and as envisaged by the Agreement.

4. SUBPROCESSORS; TRANSFER OF PERSONAL DATA

4.1. Authorised Subprocessors. Subscriber hereby grants dbt Labs general written authorisation to engage Subprocessors, as set out in the attached and incorporated Schedule 3 to Process Subscriber Personal Data.

4.2. dbt Labs will ensure that it has written agreements with the Subprocessors, which impose obligations that are no less onerous on the Subprocessor with regard to their Processing of Subscriber Personal Data as are imposed on dbt Labs under this DPA.

4.3. Changes to Subprocessors. dbt Labs shall notify the Subscriber from time to time of the changes of any Subprocessors it engages. If the Subscriber does not object within ten (10) days of receipt of the notice, the Subscriber is deemed to have accepted the new Subprocessor. Any objection by Subscriber will be written and will include reasonable detail supporting Subscriber's concern(s). If Subscriber does not object, dbt Labs may proceed with the change. If the Subscriber (acting reasonably) objects to a new Subprocessor, then without prejudice to any right to terminate the Agreement, the Subscriber may request in writing within thirty (30) days that dbt Labs move the Subscriber Personal Data to another Subprocessor and dbt Labs shall, within a reasonable time following receipt of such written request, use reasonable endeavours to ensure that the Subprocessor does not Process any of the Subscriber Personal Data. If it is not reasonably possible to use another Subprocessor, and Subscriber, acting reasonably, continues to object, either party may terminate the Agreement on thirty (30) days written notice. The rights provided in this subsection constitute the sole and exclusive remedy if Subscriber objects to any new Subprocessor.

4.4. Liability of Subprocessors. dbt Labs shall at all times remain responsible to the Subscriber for the acts and omissions of any Subprocessor as if they were the acts and omissions of dbt Labs.

4.5. Transfers of Personal Data. Before Subscriber transfers Personal Data to dbt Labs, or permits dbt Labs to access Personal Data in a jurisdiction that require SCCs, Subscriber will notify dbt Labs of the transfer, the jurisdictions and the relevant requirement(s) and the parties will work together in good faith to fulfill such requirements. With respect to any SCCs required by Data Protection Laws of the parties to permit transfers to Third Countries, the parties will negotiate in good faith to agree upon the appropriate SCC template or module and agree upon its provisions, and the appropriate template will be deemed to be executed as of the date hereof. It is not intended for any Subscriber Personal Data to be transferred outside the EEA/UK without Subscriber's express consent in the absence of the Subscribers instructions. Client understands and agrees that dbt Labs' support personnel and/or deployment engineers are globally including but not limited to locations in USA, Ireland, the United Kingdom, Germany, the Philippines, Australia, or New Zealand and may provide technical support or disaster recovery functions only via a secure connection. Subscriber acknowledges and agrees to dbt Labs processing Subscriber Personal Data out of the EEA for the limited purposes of (a) maintaining business records for financial, audit, sales, training, or regulatory purposes, and (b) when EEA support is unavailable and Subscriber either requests such processing, or has a substantial need requiring immediate assistance, dbt Labs may assist with troubleshooting or provide support to Subscriber. To the extent that the Processing of Subscriber Personal Data occurs in a Third Country by dbt Labs (acting as a data importer), dbt Labs shall, and shall procure that any of its affiliates or Subprocessors shall (as relevant), comply with the data importer's obligations set out in the Controller to Processor Clauses, which are hereby incorporated into and form part of this DPA and the Subscriber will comply with the data exporter's obligations in such Controller to Processor Clauses. Further, with respect to the Controller to Processor Clauses under the GDPR (or as adapted for the UK Addendum or for clauses issued by Swiss FADP):

4.5.1. if applicable, for the purposes of Annex I.A of such Controller to Processor Clauses, the Data Exporter is a data controller and the Data Importer is a data processor, and the name, address, contact person's details and relevant activities for each of them is as set out in the Agreement;

4.5.2. for the purposes of Appendix 1 or Annex I/I.B (as relevant) of such Controller to Processor Clauses, Schedule 1 of this DPA shall apply;

4.5.3. for the purposes of Appendix 2 of Annex II (as relevant) of such Controller to Processor Clauses, the security measures set out in Schedule 2 of this DPA shall apply; and

4.5.4. if applicable, for the purposes of: (i) Clause 7 (Docking Clause) is optional and deleted; (ii) Clause 9 of such Controller to Processor Clauses, Option 2 ("*General written authorization*") is deemed to be selected and the notice period specified in Section 4.3 of this DPA shall apply; (iii) clause 11(a) of such Controller to Processor Clauses, the optional wording in relation to independent dispute resolution is deemed to be omitted; (iv) Clause 13 (a) (First Paragraph Option) and Annex I.C, the competent supervisory authority shall be the supervisory authority of the EU member state where the Subscriber is established or where its local representative is appointed; (v) Clause 17, Option 1 is deemed to be selected and the governing law shall be Ireland and (vi) Clause 18, the competent courts shall be Ireland.

4.6. To the extent dbt Labs permits Subprocessors to Process Personal Data in any Third Country: (A) dbt Labs shall execute the Processor to Processor Clauses, if applicable, with any relevant subprocessor or subcontractor it appoints on behalf of the Subscriber; or (B) if the Processor to Processor Clauses are not applicable with any relevant Subprocessor it appoints on behalf of the Subscriber, the parties agree to execute the relevant Controller to Processor Clauses with the processing details set out in Schedule 1 of this DPA and the technical and organizational measures set out in Schedule 2 of this DPA applying for the purposes of Appendix 1 and Appendix 2 respectively.

4.7. In the event of any conflict between any terms in the Standard Contractual Clauses, this DPA and the Agreement, the Standard Contractual Clauses shall prevail.

5. COMPLIANCE, AUDITS SECURITY NOTIFICATIONS

5.1. dbt Labs Security Obligations. 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, dbt Labs shall implement and maintain or exceed appropriate technical and organisational measures on its systems to ensure a level of security appropriate to the risk, including the measures set out in Schedule 2. Subscriber shall implement and maintain or exceed appropriate technical and organisational measures on its systems to ensure a level of security appropriate to the risk.

5.2. dbt Labs Employees and Personnel. dbt Labs shall ensure that any employees or other personnel have agreed in writing to protect the confidentiality and security of Subscriber Personal Data (as applicable).

5.3. Audits. dbt Labs will, upon reasonable prior written request from the Subscriber, allow for and contribute to reasonable audits and inspections, including relevant information reasonably necessary to demonstrate Subscriber's compliance with Data Protection Laws, this DPA and/or inspections, conducted by an independent third party auditor, in possession of the required professional qualifications and bound by a duty of confidentiality provided (i) such audits or inspections are not conducted more than once per year (unless required by a Regulator); (ii) are conducted only during dbt Lab's business hours; (iii) are conducted to cause minimal disruption to dbt Labs's operations and business; (iv) are subject to dbt Labs's internal security policies; and (v) are limited to determining compliance by dbt Labs with its obligations hereunder. The Subscriber shall reimburse dbt Labs any reasonable fees or costs incurred by dbt Labs in conducting (or arranging the conduct of) any audits in accordance with this section unless dbt Labs is found by the independent auditor, acting reasonably, to be in material violation of this DPA, in which case, any reasonable fees and costs incurred by the independent auditor will be reimbursed by dbt Labs.

5.4. Security Incident Notification. If dbt Labs or any Subprocessor becomes aware of a Security Incident, dbt Labs will (a) notify the Subscriber of the Security Incident without undue delay, (b) investigate the Security Incident and provide such reasonable assistance to the Subscriber (and any law enforcement or Regulator) as required to investigate the Security Incident, and (c) take steps to remedy any noncompliance by dbt Labs with this DPA.

5.5. Subscriber Obligations. Where required by applicable Data Protection Laws, Subscriber warrants that it will issue its instructions in compliance with Data Protection Laws applicable to Subscriber as user of the Services. Notwithstanding any other provision herein, Subscriber agrees to not transfer, Process or access Personal Information or issue processing instructions (A) in violation of this Agreement or (B) that affect or may result in actions that affect any country's national security.

6. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

6.1. Data Subject Requests. Unless prohibited under applicable law, dbt Labs shall notify Subscriber of any request received by dbt Labs or any Subprocessor from a Data Subject in respect of their Personal Data included in the Subscriber Personal Data. Subscriber

authorises on its behalf, dbt Labs to respond to any Data Subject who makes a request to dbt Labs, to confirm that dbt Labs has forwarded the request to Subscriber. The parties agree that dbt Labs's forwarding Data Subjects' requests to Subscriber, in accordance with this Section, represent the scope and extent of dbt Lab's required assistance.

6.2. Data Subject Rights. Where applicable, and taking into account the nature of the Processing, dbt Labs shall use all reasonable endeavours to assist Subscriber by implementing any other appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Subscriber's obligation to respond to requests for exercising Data Subject rights laid down in applicable Data Protection Laws.

6.3. Governmental Access Requests. dbt Labs (and will make commercially reasonable endeavors to ensure its sub-processors) will not disclose Subscribers Personal Data to any governmental authority, except as necessary to comply (i) with the law or (ii) a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends dbt labs (or sub-processor) a demand for Subscriber's Personal Data, dbt labs (or its subprocessor) will attempt to (a) redirect the law enforcement agency to request that data directly from Subscriber (to effectuate, dbt labs may provide Subscriber contact information to the governmental authority), and (b) if compelled to disclose Subscriber Personal Data dbt will use commercially reasonable means to provide Subscriber notice of the demand without undue delay or as expeditiously as permitted under the circumstances to allow Subscriber to seek a protective order or other appropriate remedy unless dbt lab is advised not to by legal counsel or is legally prohibited from doing so. This section does not diminish dbt Labs' obligations under the SCCs and IDTA with respect to access by public authorities.

6.4. Disclosure. dbt Labs, Inc. is a U.S. Company headquartered in the U.S. As such, dbt Labs, Inc. is generally subject to U.S. laws, including laws which may impact dbt Labs, Inc.'s obligations pursuant to this DPA, the Standard Contractual Clauses and the IDTA. In accordance with those obligations, dbt Labs, Inc. hereby notifies Client of the following: (a) like many U.S.-based data processors, dbt Labs, Inc. may be subject to Section 702 of the U.S. Foreign Intelligence Surveillance Act, codified at 50 U.S.C. § 1881a ("FISA Section 702"), and therefore may be eligible to receive upstream or bulk surveillance orders under FISA Section 702; and (b) Executive Order 12333 ("EO 12333") does not provide the U.S. government the ability to order or demand dbt Labs, Inc. to provide assistance for the bulk collection of information and dbt Labs, Inc. will not do so voluntarily. dbt Labs, Inc. shall encrypt all transfers of personal data, which can prevent the acquisition of such data by U.S. governmental authorities pursuant to EO 12333, while that data is in transit. As of the date of this DPA, dbt Labs, Inc. has not received any requests under FISA Section 702 or EO 12333.

6.5. Cooperation. To the extent legally required, with respect to Subscriber Personal Data on its systems, dbt Labs will cooperate with Subscriber in responding to verifiable consumer requests by, for example: (a) providing responsive personal information in its possession obtained during the relationship to Subscriber; (b) deleting Subscriber Personal Data and, if applicable, notifying downstream entities about the deletion request; and (c) permitting the correction of inaccurate information.

7. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

7.1. To the extent required under applicable Data Protection Laws, dbt Labs shall provide reasonable assistance to the Subscriber with any data protection impact assessments and with any prior consultations to any Supervisory Authority of Subscriber, in each case solely in relation to Processing of Subscriber Personal Data and taking into account the nature of the Processing and information available to dbt Labs.

8. TERMINATION

8.1. Termination of this DPA is governed by the termination terms set forth in the Agreement.

8.2. Deletion of data. Personal Data received from Subscriber will be retained by dbt Labs only for so long as may be reasonably required to provide Services and comply with obligations under the Agreement. Subject to 8.3 and 8.4 below, dbt Labs shall, within ninety (90) days of the date of termination of the Agreement and Subscriber's request:

8.2.1. return a complete copy of all Subscriber Personal Data then available by secure file transfer in such a format as reasonably requested by Subscriber to dbt Labs; and

8.2.2. delete and use all reasonable efforts to procure the deletion of all other copies of Subscriber Personal Data Processed by dbt Labs or any Subprocessors; and

8.2.3. in each case cease Processing Subscriber Personal Data on behalf of the Subscriber.

8.3. Subject to section 8.4 below, Subscriber may in its absolute discretion notify dbt Labs in writing within thirty (30) days of the date of termination of the Agreement to require dbt Labs to delete and procure the deletion of all copies of Subscriber Personal Data

Processed by dbt Labs. dbt Labs shall comply without undue delay, but at least within ninety (90) days of the date of termination of the Agreement:

8.3.1. comply with any such written request; and

8.3.2. use all commercially reasonable endeavours to procure Subprocessors comply with such written request.

8.4. dbt Labs and its Subprocessors may retain Subscriber Personal Data to the extent required for legal, fiduciary, or tax purposes or for review by dbt Labs's consultants, advisors, auditors, attorneys, investors, bankers, payment processors, regulatory bodies, tax authorities, when compelled by court order, or as otherwise needed to fulfill dbt Labs's duties under this Agreement and only to the extent and for such period as required provided that dbt Labs shall ensure the confidentiality of all such Subscriber Personal Data and shall ensure that such Subscriber Personal Data is only Processed as necessary for such purpose(s) requiring its storage and for no other purpose.

9. CHANGES IN APPLICABLE DATA PROTECTION LAWS

9.1. The parties agree to negotiate in good faith modifications to this DPA if changes are required for dbt Labs to continue to process the Subscriber Personal Data as contemplated by this DPA in compliance with the Data Protection Laws or to address the legal interpretation or revision of the Data Protection Laws, including without limitation (i) any guidance on the interpretation of any of their respective provisions; (ii) the Standard Contractual Clauses or any other mechanisms or findings of adequacy are issued, invalidated or amended, or (iii) changes to adequacy rulings or the membership status of a country in the European Union or the European Economic Area.

IN WITNESS THEREOF AGREED to and SIGNED by authorized representatives of each party, as set out below:

dbt Labs, Inc.	**Subscriber: _____**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

SCHEDULE 1

DETAILS OF THE PROCESSING AND TRANSFER OF SUBSCRIBER PERSONAL DATA

Categories of data subjects whose personal data is transferred

- Authorized Users and, at the discretion of the Subscriber, any other data subjects whose data the Subscriber or its Authorized Users transforms or queries via the Platform.

Categories of personal data transferred

- Contact information, usage information, nontraditional identifiers of the Subscriber's Authorized Users, and any other Personal Data the Subscriber or its Authorized Users submit to the Platform.

- Any other Personal Data contained in any data the Subscriber or its Authorized Users transforms or queries via the Platform.

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).

- Continuous.

Nature of the processing

- The Processing of Subscriber Personal Data provided by the Subscriber to dbt Labs through the Platform or otherwise in connection with the provision of the Service.

Purpose(s) of the data transfer and further processing

- To provide the services set out in the Agreement.

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

- Until termination, as set out in clause 8 of the Agreement and this DPA.

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

- As above.

SCHEDULE 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. dbt Labs implements, maintains and enforces appropriate internal security policies and procedures, and procures that its Subprocessors do likewise, which are designed to:

a. secure any personal data Processed by dbt Labs against accidental or unlawful loss, access or disclosure;

b. identify reasonably foreseeable and internal risks to security and unauthorised access to the personal data Processed by dbt Labs;

c. minimise security risks, including through risk assessment and regular testing;

d. designate one or more employees to coordinate and be accountable for the internal security policies and procedures, and, taking into account the global distribution of dbt Labs staff, such internal security policies and procedures will manage the access allowed to the dbt Labs's network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls; and

e. meet or exceed the following additional measures:

- A SOC2 Type II annually;
- Encryption At-Rest;
- Encryption In-Transit;
- Password Requirements;
- Key Management;
- Risk Assessment;
- Vendor Risk Management;
- User Provisioning/Deprovisioning;
- Network Security;
- Vulnerability Management;
- Incident Management;
- Change Management;
- System Logging/Monitoring;
- Data Management;
- Communication;
- Business Continuity; and
- Disaster Recovery.

2. dbt Labs will, and will use reasonable efforts to procure that its Subprocessors, conduct periodic reviews of the security of their network and the adequacy of their information security program as measured against industry security standards and its policies and procedures.

3. dbt Labs will, and will use reasonable efforts to procure that its Subprocessors, periodically evaluate the security of their network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

SCHEDULE 3
AUTHORISED SUBPROCESSORS

Subprocessors	**Services provided**	**Contact Details**
Amazon Web Services	dbt Labs Cloud Platform Host for Processing Subscriber Personal Data	