virvell

DATA PROCESSING ADDENDUM

LAST UPDATED: November 2025

This Data Processing Addendum ("DPA") forms part of the Virvell Terms and Conditions, or other agreement governing the use of Virvell's services ("Agreement") entered by and between you ("you", "your", "Customer"), and Tablise Technologies Inc. ("Virvell"). This DPA sets out the terms that apply to the Processing of Personal Data (as defined below) by Virvell, on behalf of Customer, in the course of providing the Services to Customer under the Agreement.

All capitalized terms not defined herein will have the meanings set forth in the Agreement.

By using the Services, Customer accepts this DPA, and you represent and warrant that you have full authority to bind the Customer to this DPA. If you cannot, or do not agree to, comply with and be bound by this DPA, or do not have authority to bind the Customer or any other entity, please do not provide Personal Data to us.

---

1. DEFINITIONS

1.1. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. "Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Virvell, but has not signed its own Order Form with Virvell and is not a "Customer" as defined under the Agreement.

1.3. "Authorized User" means any individual authorized or otherwise enabled by Customer to use the Services through Customer's account.

1.4. "CCPA" means the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act, Cal. Civ. Code §§ 1798.100 et. seq, and its implementing regulations, as may be amended from time to time.

1.5. "Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

1.6. "Customer Data" means what is defined in the Agreement as "Customer Data."

1.7. "Data Protection Laws" means all applicable and binding privacy and data protection laws and regulations in the locations where Virvell operates the Services, including the GDPR, UK GDPR, PIPEDA, and the CCPA.

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

1.9. "GDPR" means 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.

1.10. "Information Security Standards" means the security documentation applicable to the Services purchased by Customer, as updated from time to time, as made reasonably available to Customer by Virvell.

1.11. "Personal Data" or **"Personal Information"** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with a particular Data Subject or Consumer (as defined in the CCPA, to the extent applicable), which is included in Customer Data Processed by Virvell on behalf of Customer under the Agreement, or such equivalent concept as defined under applicable Data Protection Laws.

1.12. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Virvell on behalf of Customer under the Agreement.

1.13. "Personnel" means persons authorized by Virvell to Process Customer's Personal Data.

1.14. "PIPEDA" means Canada's Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, and its implementing regulations, as may be amended from time to time.

1.15. "Process" or **"Processing"** means any operation or set of operations which is performed upon Personal Data pursuant to this DPA, whether or not by automatic means, such as collection, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.16. "Processor" means the entity which Processes Personal Data on behalf of the Controller.

1.17. "Sensitive Data" means Personal Data that is protected under a special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under applicable Data Protection Laws, which may include any of the following: (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number; (c) financial, credit, genetic, biometric or health information; (d) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences; and/or (e) account passwords in unhashed form.

1.18. "Services" means the Virvell AI-powered reference checking platform and products and services (and related Documentation) described on Customer's ordering form(s).

1.19. "Standard Contractual Clauses" means (a) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses between controllers and processors, and between processors and

processors (as applicable), as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, including all annexes thereto ("EU SCCs"); (b) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses of 21 March 2022 (version B.1.0), as incorporated into the EU SCCs through Schedule 1 Part 2 hereto ("UK Addendum"); and (c) in respect of transfers subject to the Federal Act on Data Protection (FADP – as revised as of 25 September 2020), the terms set forth in Schedule 1 Part 3 hereto ("Switzerland Addendum").

1.20. "Sub-Processor" means any third party service provider engaged by Virvell that Processes Personal Data under the instruction or supervision of Virvell.

1.21. "UK GDPR" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

---

2. DATA PROCESSING

2.1. Scope and Roles. This DPA applies when Personal Data is Processed by Virvell strictly on behalf of Customer, as part of Virvell's provision of the Services. In this context and for the purposes of the GDPR or any similar Data Protection Laws, Customer is the data Controller and Virvell is the data Processor (or such other similar terms as defined under applicable Data Protection Laws); and for the purposes of the CCPA (to the extent applicable), Customer is the Business and Virvell is the Service Provider.

2.2. Subject Matter, Duration, Nature and Purpose of Processing. Virvell Processes Customer's Personal Data as part of providing Customer with the Services, pursuant to the specifications and for the duration under the Agreement.

2.3. Type of Personal Data and Categories of Data Subjects. Customer and Authorized Users determine the identity of the persons which are part of the reference check conversations analyzed by the Services, and the type and nature of any Personal Data (if any) exchanged in such conversations or included in such content. Virvell has no control over the identity of the Data Subjects whose Personal Data is processed on behalf of Customer and over the types of Personal Data Processed.

Types of Personal Data processed may include:

- Contact information (names, phone numbers, email addresses)
- Employment information (job titles, employment dates, work history)
- Voice recordings and conversation transcripts
- Performance assessments and professional feedback
- Reference recommendations and evaluations

Categories of Data Subjects may include:

- Job candidates undergoing reference checks
- Professional references (current and former colleagues, supervisors)
- Customer employees (hiring managers, HR personnel)

The Services are not intended for the Processing of Sensitive Data beyond what is necessary for employment verification purposes. At Customer's selection, the Services may also be used to capture voice identifiers relating to Authorized Users and reference providers, for conversation analysis and report generation purposes.

2.4. Customer's Obligations and Instructions. Customer shall, in its use of the Services, only submit or otherwise have Personal Data Processed in accordance with the requirements of Data Protection Laws. Virvell will only Process Personal Data on behalf of and in accordance with Customer's reasonable instructions.

Customer instructs Virvell to Process Personal Data for the following purposes:

(i) Processing to provide and ensure proper operation of the Services in accordance with the Agreement;

(ii) Processing initiated or instructed by Authorized Users in their use of the Services;

(iii) Processing to comply with other reasonable instructions provided by Customer where such instructions are consistent with the Agreement;

(iv) sharing Personal Data with, or receiving Personal Data from, third parties in accordance with Customer's instructions and/or pursuant to Customer's use of the Services (e.g., integrations between the Services and any services provided by third parties, as configured by or on behalf of Customer);

(v) rendering Personal Data fully and irrevocably anonymous and non-personal, in accordance with applicable standards recognized by Data Protection Laws and guidance issued thereunder; and

(vi) Processing as required under any applicable laws to which Virvell is subject, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that Virvell shall inform Customer of the legal requirement before Processing, unless prohibited under such law or requirement.

For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

Where required by applicable data protection laws, Customer shall:

- Configure and utilize any consent management features of the Services
- Ensure lawful recording, processing, and use of audio communications
- Provide all necessary notices to relevant Data Subjects, including a description of the Services

- Secure all necessary permissions and consents, or other applicable lawful grounds for Processing Personal Data pursuant to this DPA and/or under Data Protection Laws

Customer shall indemnify, defend and hold harmless any claim, damages or fine against Virvell arising from any failure to acquire or use the Personal Data with legal consent or legitimate business purpose or in violation of any Data Protection Laws.

Virvell will inform Customer, if in Virvell's opinion an instruction infringes any provision under any Data Protection Laws and will be under no obligation to follow such instruction, until the matter is resolved in good-faith between the parties.

To the extent that Virvell cannot comply with an instruction from Customer, (i) Virvell shall promptly inform Customer, providing relevant details of the problem, (ii) Virvell may, without any kind of liability to Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) and/or suspend access to the Customer's account, and (iii) if the parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing. Customer will have no further claims against Virvell (including, without limitation, requesting refunds for the Services) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

2.5. CCPA Standard of Care; No Sale or Sharing of Personal Information. Virvell acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that Virvell provides to Customer under the Agreement. As may be applicable to the Services provided under the Agreement, Virvell certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling or sharing (as such terms are defined in the CCPA) any Personal Information Processed hereunder, without Customer's prior written consent or instruction, nor take any action that would cause any transfer of Personal Information to or from Virvell under the Agreement or this DPA to qualify as "selling" and/or "sharing" such Personal Information under the CCPA.

Virvell acknowledges that Customer discloses Personal Information to Virvell only for limited and specified business purposes (as such term is defined in the CCPA) set out in this DPA and the Agreement. Virvell shall process all Personal Information only (i) for such limited and specific business purpose(s), and (ii) in compliance with applicable sections of the CCPA, in a manner that provides the same or materially similar level of privacy protection as required of Customer considering the Personal Information processed and industry standards.

Virvell shall not (i) retain, use, or disclose Personal Information outside the direct business relationship of the parties, as described in the Agreement, or for any business or commercial purpose other than for the specific business purpose of performing the Services or as otherwise permitted by the Agreement and/or this DPA, nor (ii) combine Personal Information with personal information Virvell processes on behalf of other parties unless expressly permitted under the CCPA and the Agreement between the parties.

As applicable to the Services provided, Virvell shall implement reasonable security measures, as described in Section 7 of this DPA, as appropriate under the CCPA, and reasonably assist Customer or otherwise enable Customer to comply with its obligations relating to any request received from an individual under the CCPA, as

described in Section 3 of this DPA. Customer shall inform Virvell of any request received from an individual under the CCPA which requires Virvell's assistance in order to be fulfilled by Customer, and shall provide Virvell all information necessary for it to assist with the request.

Subject to the audit provisions in the Agreement and this DPA, Virvell acknowledges that Customer has the right to take reasonable and appropriate steps to ensure that Virvell uses Personal Information in a manner consistent with Customer's obligations under the CCPA. Virvell further acknowledges that Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information by Virvell, subject to the conditions agreed upon in this DPA, including audit provisions. Virvell shall notify Customer if Virvell makes a determination that it can no longer meet its obligations under the CCPA.

---

3. ASSISTANCE

Taking into account the nature of the Processing, Virvell will reasonably assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the Data Subjects' rights under the GDPR, PIPEDA or other Data Protection Laws, to request access, rectification or deletion of Personal Data, to restrict or object to further processing of such data, to receive a portable copy thereof, or to request not to be subject to automated individual decision-making.

Virvell will further reasonably assist Customer, upon Customer's reasonable request, in ensuring compliance with Customer's obligations in connection with the security of Processing, notification of a Personal Data Breach to supervisory authorities and affected Data Subjects, Customer's data protection impact assessments and Customer's prior consultation with supervisory authorities, insofar as it relates to Virvell's Processing of Personal Data under this DPA, and to the extent Customer does not otherwise have access to the relevant information, and that such information is available to Virvell.

Except for negligible costs, Customer will promptly reimburse Virvell with costs and expenses incurred by Virvell in connection with the provision of assistance to Customer under this DPA.

---

4. VIRVELL PERSONNEL

4.1. Limitation of Access. Virvell will ensure that Virvell's access to Personal Data is limited to those Personnel who require such access to perform the Agreement.

4.2. Confidentiality. Virvell will impose appropriate contractual obligations upon its Personnel engaged in the Processing of Personal Data, including relevant obligations regarding confidentiality, data protection, and data security. Virvell will ensure that its Personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training in their responsibilities, and have

executed written confidentiality agreements. Virvell will ensure that such confidentiality agreements survive the termination of the employment or engagement of its Personnel.

---

5. SUB-PROCESSORS

5.1. Authorization. Virvell may engage Sub-Processors to Process Personal Data on behalf of Customer. Customer hereby provides Virvell with a general authorization to engage the Sub-Processors listed at **https://www.virvell.ai/sub-processors/**.

Current Sub-Processors include:

Sub-Processor	Service Provided	Location
AI Language Services Provider	Natural language processing and conversation analysis	United States
Voice Processing Provider	Voice call transcription and processing	United States
Stripe, Inc.	Payment processing	United States
Salesforce (Heroku)	Cloud hosting infrastructure	United States
Twilio Inc. (SendGrid)	Email delivery and notifications	United States

All Sub-Processors have entered into written agreements with Virvell that bind them by data protection obligations substantially similar to those under this DPA. Where a Sub-Processor fails to fulfil its data protection obligations in connection with the Processing of Personal Data under this DPA, Virvell will remain fully liable to Customer for the performance of that Sub-Processor's obligations.

5.2. New Sub-Processors. Virvell may engage with a new Sub-Processor ("New Sub-Processor") to Process Personal Data on Customer's behalf. Virvell's webpage accessible via https://www.virvell.ai/sub-processors offers a mechanism to subscribe to notifications of new Sub-Processors, to which Customer may subscribe.

Virvell shall provide notification of any new Sub-Processor(s) before authorizing such new Sub-Processor(s) to Process Personal Data in connection with the provision of the Services. Customer may object to the Processing of Customer's Personal Data by the New Sub-Processor, for reasonable and explained grounds, by providing a written objection to **privacy@virvell.ai** within 5 business days following Virvell's written notice to Customer of the intended engagement with the New Sub-Processor.

If Customer timely sends Virvell a written objection notice, the parties will use good-faith efforts to resolve Customer's objection. In the absence of a resolution, Virvell will use commercially reasonable efforts to provide Customer with the same level of service, without using the New Sub-Processor to Process Customer's Personal Data.

---

6. CROSS-BORDER DATA TRANSFERS

6.1. Transfers from the EEA, Switzerland, or the United Kingdom, to countries that offer adequate level of data protection. Personal Data may be transferred from EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "EEA"), Switzerland, or the United Kingdom ("UK"), to countries that offer an adequate level of data protection pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission, or Switzerland, or the UK as relevant ("Adequacy Decisions"), as applicable, without any further safeguard being necessary.

6.2. Transfers from the EEA, Switzerland or the United Kingdom to DPF-certified organizations in the USA. Personal Data may be transferred from the EEA, Switzerland or the UK to organizations in the United States of America ("USA") certified under the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, or the Swiss-US Data Privacy Framework (as applicable) (collectively, "DPF"), without the need for additional safeguards. To the extent Personal Data from the EEA, Switzerland or the UK is transferred to and processed by Virvell in the USA on the basis of Virvell's certification to the DPF, and the Parties can no longer rely on the DPF, Section 6.3 of this DPA shall apply.

6.3. Transfers from the EEA, Switzerland, or the United Kingdom, to other countries. If the Processing of Personal Data by Virvell includes transfers (either directly or via onward transfer) from the EEA ("EEA Transfer"), Switzerland ("Swiss Transfer"), or the UK ("UK Transfer") to other countries which have not been subject to a relevant Adequacy Decision ("Cross-Border Transfer"), and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Virvell for the lawful transfer of personal data (as defined in the GDPR) outside the EEA, Switzerland, or the UK, as applicable, then (i) the terms set forth in Part 1 of Schedule 1 (EEA Cross Border Transfers) shall apply to any such EEA Transfer; (ii) the terms set forth in Part 2 of Schedule 1 (UK Cross Border Transfers) shall apply to any such UK Transfer; (iii) the terms set forth in Part 3 of Schedule 1 (Switzerland Cross Border Transfers) shall apply to any such Swiss Transfer; and (iv) the terms set forth in Part 4 of Schedule 1 (Additional Safeguards) shall apply to any such Cross-Border Transfers.

6.4. Additional Transfers. If the Processing performed by Virvell includes a transfer of Personal Data by Customer, or mandated by Customer, from any other jurisdiction which mandates a particular compliance mechanism for the lawful transfer of such data be established, Customer shall notify Virvell of such applicable requirements, and the Parties may seek to make any necessary amendments to this DPA in accordance with the provisions of Section 14 below.

---

7. SECURITY

7.1. Controls. Virvell will implement and maintain administrative, physical and technical safeguards designed for the protection of the security, confidentiality and integrity of Customer's Personal Data, pursuant to the Virvell Information Security Standards. Virvell regularly monitors its compliance with these safeguards. Virvell will not materially decrease the overall security of the Services during the term of the Agreement.

Security measures include:

- Encryption of data in transit (TLS 1.2+) and at rest (AES-256)
- Access controls and multi-factor authentication
- Regular security assessments and vulnerability testing
- Incident response procedures and breach notification protocols
- Employee confidentiality agreements and security training
- Secure development practices and code review processes
- Regular backups and disaster recovery procedures
- Network security and intrusion detection systems

7.2. Policies, Certifications and Audit Reports. Virvell uses external auditors to verify the adequacy of its security measures. Upon Customer's written request at reasonable intervals and subject to confidentiality limitations, Virvell will make available to Customer that is not a Virvell competitor (or to a third party auditor on Customer's behalf, that is not a Virvell competitor and subject to the auditor's execution of Virvell's non-disclosure agreement), security documentation and certifications commonly made available to Virvell Customers.

---

8. PERSONAL DATA BREACH MANAGEMENT AND NOTIFICATION

8.1. Breach Notification. Virvell will maintain security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer's Personal Data being Processed hereunder by Virvell or any of Virvell's Sub-Processors.

Virvell's notice will at least: (a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) communicate the name and contact details of a designated officer on Virvell's data protection team, which will be available to provide any additionally available information about the Personal Data Breach;

(c) describe the likely consequences of the Personal Data Breach;

(d) describe the measures taken or proposed to be taken by Virvell to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

8.2. Customer Communications. Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Personal Data Breach which directly or indirectly identifies Virvell (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Virvell's prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable Data Protection Laws. In the latter case, unless prohibited by such laws, Customer shall provide Virvell with reasonable prior written notice to provide Virvell with the opportunity to object to such disclosure and in any case, Customer will limit the disclosure to the minimum scope required by such laws.

---

9. AUDIT AND DEMONSTRATION OF COMPLIANCE

9.1. Information Provision. Virvell will make available to Customer, pursuant to Customer's reasonable written request, all information necessary for Customer to demonstrate compliance with its obligations under applicable Data Protection Laws and this DPA, in relation to the Processing of Personal Data under this DPA by Virvell and its Sub-Processors. Such information shall only be used by Customer to assess compliance with the aforesaid obligations, and may not be disclosed to any third party without Virvell's prior written approval. As soon as the purpose of such information is met, Customer will permanently dispose of all copies thereof.

9.2. Audit Rights. Virvell will allow for and contribute to audits, including inspections, conducted by Customer or a reputable auditor mandated by Customer (who are each not a competitor of Virvell or affiliated with such a competitor), to assess Virvell's compliance with its obligations under this DPA. Virvell may satisfy the audit obligation under this section by providing Customer with attestations, certifications and summaries of audit reports conducted by accredited third party auditors.

Audits by Customer are subject to the following terms:

(i) the audit will be pre-scheduled in writing with Virvell, at least 45 days in advance and will be performed not more than once a year (except for an audit following a Personal Data Breach);

(ii) the auditor will execute a non-disclosure and non-competition undertaking toward Virvell;

(iii) the auditor will not have access to non-Customer data;

(iv) Customer will make sure that the audit will not interfere with or damage Virvell's business activities and information and network systems;

(v) Customer will bear all costs and assume responsibility and liability for the audit;

(vi) no audit shall include access to Virvell's network and/or networks that contain Virvell's customer data;

(vii) Customer will receive only the auditor's report, without any Virvell 'raw data' materials, and will keep the audit results in strict confidence and will use them solely for the specific purposes of the audit under this section;

(viii) at the request of Virvell, Customer will provide it with a copy of the auditor's report; and

(ix) as soon as the purpose of the audit is completed, Customer will permanently dispose of the audit report.

---

10. RETURN OR DELETION OF PERSONAL DATA

Upon 30 days following termination or expiration of the Agreement, Virvell shall delete all Customer Data in its possession or control, except for:

(a) Voice recordings, which shall be retained for 3 years from the date of collection as disclosed in Virvell's Privacy Policy;

(b) Reference check reports and decisions, which shall be retained for 4 years from the date of generation as disclosed in Virvell's Privacy Policy; and

(c) Customer Data that Virvell is required by applicable law to retain, or Customer Data archived on back-up systems (e.g., in the form of audit logs), which Customer Data Virvell shall securely isolate and protect from any further Processing, except to the extent required by applicable law.

---

11. DISPUTE RESOLUTION

The parties will attempt in good faith to resolve any dispute related to this DPA as a precondition to commencing legal proceedings, first by direct communications between the persons responsible for administering this DPA and next by negotiation between executives with authority to settle the controversy.

Either party may give the other party a written notice of any dispute not resolved in the normal course of business. Within five business days after delivery of the notice, the receiving party will submit to the other party a written response. The notice and the response will include a statement of each party's position and a summary of arguments supporting that position and the name and title of the executive who will represent that party.

Within five business days after delivery of the disputing party's notice, the executives of both parties will meet at a mutually acceptable time and place, including by phone, and thereafter as often as they reasonably deem necessary, to resolve the dispute. All reasonable requests for information made by one party to the other will be honored. All negotiations pursuant to this clause are confidential and will be treated as compromise and settlement negotiations for purposes of applicable rules of evidence.

12. TERM

This DPA will commence and become legally binding on the earlier of (i) the date of its execution, (ii) the effective date of the Agreement to which it relates, or (iii) the initiation of Virvell's Processing of Personal Data on behalf of Customer; and will continue until the Agreement expires or is terminated.

13. AUTHORIZED AFFILIATES

13.1. Contractual Relationship. The parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate agrees to be bound by the Customer's obligations under this DPA, if and to the extent that Customer Processes Personal Data on the behalf of such Authorized Affiliates, thus qualifying them as the "Controller". All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.

13.2. Communication. The Customer shall remain responsible for coordinating all communication with Virvell under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

14. MODIFICATIONS

Each party may by at least 45 days' prior written notice to the other party, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under, any Data Protection Laws, to allow Processing of Customer Personal Data to be made (or continue to be made) without breach of that Data Protection Law.

Pursuant to such notice: (a) Virvell shall make commercially reasonable efforts to accommodate such modification requested by Customer or that Virvell believes is necessary; and

(b) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Virvell to protect Virvell against additional risks, or to indemnify and compensate Virvell for any further steps and costs associated with the variations made herein at Customer's request.

The parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's or Virvell's notice as soon as is reasonably practicable. In the event that the parties are unable to reach such

an agreement within 30 days of such notice, then Customer or Virvell may, by written notice to the other party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which are affected by the proposed variations (or lack thereof). Customer will have no further claims against Virvell (including, without limitation, requesting refunds) pursuant to the termination of the Agreement and the DPA as described in this Section.

---

15. LIMITATION OF LIABILITY

15.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates of Customer and Virvell, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

15.2. For the avoidance of doubt, Virvell's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates and Customer Representatives arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and its Authorized Affiliates and Customer Representatives and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

15.3. Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its schedules and appendices.

---

16. CONFLICT

16.1. In the event of any conflict or inconsistency between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

16.2. In the event of any conflict between certain provisions of this DPA and any of its Schedules and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

---

17. CONTACT INFORMATION

For any questions or concerns regarding this DPA or data protection matters, please contact:

Tablise Technologies Inc. (Virvell)
18 King Street East, Suite 1400
Toronto, ON M5C 1C4
Canada

Email: privacy@virvell.ai
Legal: legal@virvell.ai

SCHEDULE 1 – CROSS BORDER TRANSFERS

PART 1 – EEA CROSS BORDER TRANSFERS

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to an EEA Transfer.

2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Personal Data and Virvell is the data processor of the Personal Data.

3. Module Three (Processor to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data processor of the Personal Data and Virvell is a Sub-processor of the Personal Data.

4. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.

5. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the Standard Contractual Clauses shall apply, and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in Section 5.2 of the DPA.

6. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply.

7. In Clause 17 of the Standard Contractual Clauses, Option 1 shall apply, and the Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Province of Ontario, Canada.

8. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of Ontario, Canada.

9. **Annex I.A** of the Standard Contractual Clauses shall be completed as follows:

Data Exporter: Customer.

Contact details: As detailed in the Agreement.

Data Exporter Role:

- Module Two: The Data Exporter is a data controller.
- Module Three: The Data Exporter is a data processor.

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

Data Importer: Virvell (Tablise Technologies Inc.).

Contact details: Tablise Technologies Inc.
18 King Street East, Suite 1400
Toronto, ON M5C 1C4, Canada
Email: privacy@virvell.ai

Data Importer Role:

- Module Two: The Data Importer is a data processor.
- Module Three: The Data Importer is a sub-processor.

Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

10. **Annex I.B** of the Standard Contractual Clauses shall be completed as follows:

Categories of data subjects:

- Job candidates undergoing reference checks
- Professional references (current and former colleagues, supervisors)
- Customer employees (hiring managers, HR personnel)

Types of Personal Data:

- Contact information (names, phone numbers, email addresses)
- Employment information (job titles, employment dates, work history)

- Voice recordings and conversation transcripts
- Performance assessments and professional feedback
- Reference recommendations and evaluations

Sensitive Data: The Parties do not intend for Sensitive Data to be transferred beyond what is necessary for employment verification purposes.

Frequency of transfer: Continuous basis for the duration of the Agreement.

Nature and purpose of Processing:

- Conducting automated voice reference checks
- Transcribing and analyzing reference conversations
- Generating employment verification reports
- Quality assurance and compliance monitoring
- Improving AI models through anonymized data analysis

Retention period:

- Voice recordings: 3 years from date of collection
- Reference reports: 4 years from date of generation
- Account data: Duration of Agreement plus 24 months
- Other data: As specified in the Agreement and Privacy Policy

Sub-processors: In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth in Section 5 of the DPA.

11. **Annex I.C** of the Standard Contractual Clauses shall be completed as follows:

The competent supervisory authority in accordance with Clause 13 is the Office of the Privacy Commissioner of Canada.

12. The information security standards referred to in Section 7 of the DPA serves as Annex II of the Standard Contractual Clauses.

13. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses will prevail.

PART 2 – UK CROSS BORDER TRANSFERS

Table 1: The Parties: as detailed in Section 9 of Part 1 of this Schedule 1.

Table 2: Selected SCCs, Modules and Selected Clauses: as detailed in Part 1 of this Schedule 1.

Table 3: Appendix Information: means the information which must be provided for the selected modules as set out in the Appendix of the Standard Contractual Clauses (other than the Parties), and which is set out in Part 1 of this Schedule 1.

Table 4: Ending this addendum when the Approved Addendum Changes: neither Party may end this Addendum as set out in Section 19 of this Part 2.

The Alternative Part 2 Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office (ICO) and laid before the UK Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those mandatory clauses.

PART 3 – SWITZERLAND CROSS BORDER TRANSFERS

The Parties agree that the Standard Contractual Clauses as detailed in Part 1 of this Schedule 1, shall be adjusted as set out below where the Federal Act on Data Protection of 25 of September 2020 (the "FADP") applies to Switzerland Transfers:

1. References to the Standard Contractual Clauses means the Standard Contractual Clauses as amended by this Part 3;

2. The Swiss Federal Data Protection and Information Commissioner ("FDPIC") shall be the sole Supervisory Authority for Switzerland Transfers exclusively subject to the FADP;

3. The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the Standard Contractual Clauses shall be interpreted to include the FADP with respect to Switzerland Transfers.

4. References to Regulation (EU) 2018/1725 are removed.

5. Switzerland Transfers subject to both the FADP and the GDPR, shall be dealt with by the FDPIC, insofar as the Switzerland Transfer is governed by the FADP, and by the EU Supervisory Authority named in Part 1 of this Schedule 1, insofar as the Switzerland Transfer is governed by the GDPR;

6. References to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses;

7. Where Switzerland Transfers are exclusively subject to the FADP, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP;

8. Where Switzerland Transfers are subject to both the FADP and the EU GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP insofar as the Switzerland Transfers are subject to the FADP;

PART 4 – ADDITIONAL SAFEGUARDS

1. In the event of any Cross-Border Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:

a. The Data Importer shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from the Data Exporter to the Data Importer and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit and at rest intended to deny attackers the ability to read data.

b. The Data Importer will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under GDPR, FADP, PIPEDA or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Act ("FISA");

c. If the Data Importer becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Customer's Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:

I. The Data Importer will notify the Data Exporter immediately after first becoming aware of such demand for access to Customer's Personal Data and provide the Data Exporter with all relevant details of the same, unless and to the extent legally prohibited to do so;

II. The Data Importer shall inform the relevant government authority that the Data Importer is a processor of the Customer's Personal Data and that the Data Exporter and/or Controller has not authorized the Data Importer to disclose the Customer's Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to the Customer's Personal Data should therefore be notified to or served upon the Data Exporter and/or Controller in writing;

III. The Data Importer will use commercially reasonable legal mechanisms to challenge any such demand for access to Customer's Personal Data which is under the Data Importer's control. Notwithstanding the above, (a) the Data Exporter acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Customer's Personal Data, the Data Importer has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection (c)(III) shall not apply. In such event, the Data Importer shall notify the Data Exporter, as soon as possible, following the access by the

government authority, and provide the Data Exporter with relevant details of the same, unless and to the extent legally prohibited to do so.

2. Once in every 12-month period, the Data Importer will inform the Data Exporter, at the Data Exporter's written request, to the extent permitted by applicable law, of the types of binding legal demands for Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.