Data Processing Agreement

1. Definitions

1.1. **Agreement** means the standard terms and conditions entered into between you as the "**Customer**" and us as the Licensor (as defined in the Agreement).

1.2. **Data Protection Legislation** means all data protection and privacy legislation applying to you and/or us which is in force from time to time. This may include (to the extent applicable) the Australian Privacy Act 1988 (Cth); the EU's General Data Protection Regulation (2016/679) (**GDPR**); the GDPR as defined in section 3(10) (as supplemented by section 205(4)) of the DPA 2018 (**UK GDPR**); the UK's Data Protection Act 2018 (**DPA 2018**); and applicable U.S. state privacy laws including the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations, as amended by the California Privacy Rights Act.

1.3. **Controller**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Processor**, **Processing/Process/Processed** and **Supervisory Authority** are as defined in the GDPR.

1.4. **Data Transfer Provisions** means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Decision (EU) 2021/914 2021 (**EU SCCs**) and the UK International Transfer Addendum to the EU SCCs (**UK Addendum**).

1.5. **FADP** means the Swiss Federal Act on Data Protection.

1.6. **Services** means the services which we provide to you under the Agreement.

2. Description of Processing

2.1. The parties acknowledge that this Data Processing Agreement (**DPA**) applies only to the Personal Data we are Processing on our Customer's instructions, and in connection with such Processing:

2.1.1. **Roles**: We act as the Customer's Processor in our provision of the Services;

2.1.2. **Categories of Personal Data**: In the provision of Services to the Customer, the categories of Personal Data we process are Customer Data as defined in the Agreement (including name, phone number and email address), and other Personal Data as defined in the Agreement provided to us directly by the individual applying for employment with you, such as in response to the

interview questions asked of the individual during our provision of the Services, which may include special categories of Personal Data such as Data Subjects' age, health, and racial or ethnic origin;

2.1.3. **Categories of Data Subjects**: In the provision of Services to you, the categories of Data Subjects whose Personal Data we process are employees or individuals applying for employment with you (**Candidates**); and

2.1.4. **Nature and Purposes of Processing**: The processing is carried out to enable us to provide the Services to you during the term of the Agreement, being to:

i. collect Candidates' responses to the interview questions you set and your requests for information about Candidates' qualifications and experience, for us to then provide scores and recommendations to you for you to determine a Candidate's suitability for a position;
ii. collect Candidates' responses to your questions for your own diversity and inclusion monitoring (if any); and
iii. provide you with reports such as Candidates' satisfaction with the interview process, their time taken to complete each section of the interview and plagiarism rate.

2.2. During the term of the Agreement, both parties anticipate they will exchange Personal Data acting as independent controllers relating to their employees as necessary in connection with matters such as the negotiation of subsequent SOWs and account management. Each party will process such Personal Data in accordance with their own privacy notice. Our privacy notice is available at: https://sapia.ai/privacy-policy/.

2.3. You hereby agree to us Processing Customer Data to de-identity it for the purposes of the Data Protection Legislation, for us to use that de-identified data (that no longer includes Personal Data) for the purposes of developing and improving our services, including:

i. using de-identified data about Candidates' experiences of the interview process to promote our services (it will also not be possible to identify you as our Customer from the data we publish unless we obtain your permission in advance);

ii. using de-identified data about Candidates' location, age, gender, health, and racial and ethnic origin, for the purposes of testing for bias in our services as required by the EU's Artificial Intelligence Act and other relevant legislation;

iii. using Candidates' de-identified responses to interview questions to train our AI algorithms to improve our AI model; and

iv. using both de-identified data sets in in (ii) and (iii) above to contribute to scientific research.

3. Your Obligations

3.1. You retain control of the Personal Data we are processing on your behalf and remain responsible for your compliance obligations under the applicable Data Protection Legislation. Such obligations include providing any required notices and obtaining any required consents, and for the Processing instructions provided to us.

3.2. You warrant and represent that our expected use of the Personal Data as set out in this Agreement will comply with the Data Protection Legislation.

4. Our Obligations

4.1. We will only Process the Personal Data to the extent, and in such a manner, as is necessary for providing the Services in accordance with this Agreement and your instructions. We will not Process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. We will immediately notify you if, in our opinion, your instruction would not comply with the Data Protection Legislation or if we determine we can no longer meet our obligations under the Data Protection Legislation.

4.2. We will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless you or this Agreement specifically authorises the disclosure, or it is required by applicable law. If a law, court, regulator, or Supervisory Authority requires us to process or disclose Personal Data, we will first use our reasonable endeavours to inform you of the legal or regulatory requirement and give you an opportunity to object or challenge the requirement, unless applicable law prohibits such notice.

4.3. We will reasonably assist you with meeting your compliance obligations under the Data Protection Legislation, considering the nature of our Processing and the information available to us, including in relation to Data Subjects' rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

4.4. We will not sell for monetary or other valuable consideration, share for purposes of cross-context behavioral advertising, or otherwise disclose, Customer Data to third parties except as permitted under paragraph 8. We will not use Customer Data outside of the direct business relationship between us and you as our Customer unless permitted by the Data Protection Legislation, and will not

combine Customer Data with the personal data we receive from or on behalf of another customer or collect from our own interactions with Data Subjects. We may Process Customer Data as reasonably necessary for the following business purposes: (i) providing the Services, (ii) helping to ensure security and integrity of the Services, to the extent the use of the Customer Data is reasonably necessary and proportionate for those purposes, (iii) debugging to identify and repair errors that impair existing intended functionality of the Services, (iv) undertaking internal research for technological development and demonstration, and (v) undertaking activities to verify or maintain the quality of the Services. The Customer discloses the Customer Data only for the performance of these limited and specified business purposes, and we may not retain, use, or disclose the Customer Data for any other business or commercial purpose, unless permitted by the Data Protection Legislation.

5. Security

5.1. We will ensure that all our employees and contractors are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data.

5.2. We will always implement appropriate technical and organisational measures against unauthorised or unlawful Processing, access, disclosure, copying, modification, storage, reproduction, display, or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure, or damage of Personal Data. We will maintain an up-to-date written record of our then-current security measures, which we shall provide to you on request, and review at least on a quarterly basis to ensure they remain current and complete. We may update our security measures from time to time, provided they do not result in a reduction in the security over the Personal Data to which they apply.

5.3. We will implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate the pseudonymisation and encryption of Personal Data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6. Personal Data Breach

6.1. Without undue delay, we will notify you if we become aware of any Personal Data Breach relating to you or your Candidate's Personal Data.

6.2. Where we become aware of an event within the scope of paragraph 6.1, we shall, without undue delay, also provide you with any additional information in

connection with the event reasonably requested by you which we are able to obtain and which is permitted to be disclosed by law enforcement.

6.3. Immediately following any unauthorised or unlawful Personal Data Processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. We will reasonably co-operate with you in your handling of the matter.

6.4. We will not inform any third party of any Personal Data Breach without first obtaining written consent from you, except when required to do so by law.

6.5. You have the sole right to determine whether to provide notice of and remedies in connection with the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation.

7. Cross-border Transfers of Personal Data

7.1. If an adequate protection measure for the international transfer of Personal Data is required under applicable Data Protection Legislation (and has not otherwise been arranged by the parties) the Data Transfer Provisions shall be incorporated into this DPA in the International Transfers Appendix as if they had been set out in full.

7.2. Where a transfer of Personal Data would be an internal transfer under the FADP, the Data Transfer Provisions shall apply pursuant to paragraph 7.1, however:

7.2.1. the term '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 (Switzerland) in accordance with Clause 18(c.) of the EU SCCs;

7.2.2. references to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP;

7.2.3. the EU SCCs also protects the data of legal entities until the entry into force of the revised FADP; and

7.2.4. the competent Supervisory Authority (for purposes of Annex 1.C (under Clause 13 of the EU SCCs)) shall be the Federal Data Protection and Information Commissioner (FDPIC) insofar as the data transfer is governed by the FADP, and the EU authority specified in Annex 1.C insofar as the data transfer is governed by the GDPR.

8. Subprocessors

8.1. We may only authorise a third party (subprocessor) to process the Personal Data if:

8.1.1. You are provided with an opportunity to object to the appointment of each subprocessor within ten (10) days of us providing you with reasonable details of the forthcoming changes to our subprocessors, with such details to be provided by us;

8.1.2. We enter into a written contract with the subprocessor that contains terms which comply with Data Protection Legislation, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon your written request and at your expense, provide you with copies of such contracts (subject to redaction of any confidential information); and

8.1.3. We maintain control over all Personal Data we entrust to the subprocessor.

8.2. You authorise us to use the subprocessors set out on our dedicated subprocessor webpage available at https://sapia.ai/subprocessors/ (which provide support to us in the general categories of data storage, hosting (including data centres and providers of virtual software environments) and IT support).

8.3. Where the subprocessor fails to fulfil its obligations under such written agreement, we remain fully liable to you for the subprocessor's performance of its agreement obligations.

9. Complaints, Data Subject Requests and Third-Party Rights

9.1. We will, at your cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to you as you may reasonably require, to enable you to comply with:

9.1.1. the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data, or any other right to which the Data Subject is entitled under the Data Protection Legislation; and

9.1.2. information or assessment notices served on you by any supervisory authority under the Data Protection Legislation.

9.2. Where required by the Data Protection Legislation, we will notify you promptly if we receive any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation. Where appropriate, we will inform the sender that they need to contact you directly.

9.3. In the event we receive a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation, you authorise us to provide an acknowledgement to the Data Subject directly, and to inform the Data Subject that they need to contact you directly.

9.4. We will give you our full co-operation and assistance in responding to any complaint, notice, communication, or Data Subject request.

10. Data Return and Destruction

10.1. At your request, we will give you a copy of or access to all or part of the Customer's Personal Data in its possession or control in a commonly accessible and electronic format determined by us.

10.2. On termination of the Services for any reason or expiry of its term, we will promptly and securely delete, de-identify, destroy, or, if directed in writing by you, return and not retain, all or any Personal Data we are processing on your behalf under this DPA in our possession or control. This requirement shall not apply to Personal Data which we have archived on our backup systems which are not reasonably accessible, provided that such Personal Data is deleted promptly in the event such backups become reasonably accessible (such as by us using those backups to restore its systems).

10.3. Paragraph 10.2 shall not apply to the extent any law, regulation, or government or regulatory body requires us to retain any documents or materials that we would otherwise be required to return or destroy.

11. Records

11.1. We will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data we carry out on your behalf ("**Records**") and provide you with copies of the Records upon request.

12. Audit

12.1. No more than once during any consecutive twelve (12) month period, on request from you, we will provide you with the relevant information from our audit (which may have been carried out internally or by third-party representatives) to evidence our compliance with this DPA and provide the results to you. You shall be entitled to ask questions of us related to compliance with Data Protection Legislation in advance of the audit, which we shall use our reasonable endeavours to respond to adequately when providing the audit results. Upon your reasonable request we will make available all information in our possession reasonably necessary to demonstrate our compliance with the Data Protection Legislation.

12.2. On your written request and at your cost, we will exercise relevant audit rights we have in connection with our subprocessors' compliance with their obligations regarding your Personal Data and provide you with the audit results.

12.3. The audit rights set out at paragraphs 12.1 – 12.2 are your only contractual rights (and our only contractual obligations) in connection with the auditing of our Processing of Personal Data. Save that nothing in this DPA shall prevent or is intended to undermine the rights and powers granted to Data Subjects or Supervisory Authorities, and accordingly we shall submit to any audits required by a Supervisory Authority or Data Protection Legislation.

International Transfers Appendix

Part A: Standard Contractual Clauses

To the extent a restricted transfer of Personal Data is made pursuant to the GDPR, this Part A and the following terms shall apply:

(i) Module One of the Standard Contractual Clauses if you, acting as a Controller, are making a restricted transfer of Personal Data subject to the GDPR to us, acting as a Controller.

(ii) Module Two of the Standard Contractual Clauses if you, acting as a Controller, are making a restricted transfer of Personal Data subject to the GDPR to us, acting as a Processor.

Supplementary clauses to the Standard Contractual Clauses

Provision of information: To the extent Module 1 of the EU SCCs applies for the purposes of Clause 8.2 of the EU SCCs and to enable Data Subjects to effectively exercise their rights, the parties have agreed that the exporter shall inform Data Subjects of the information required and Clause 8.3 of the EU SCCs the parties hereby agree that the exporter shall be primarily responsible for ensuring that Personal Data is accurate and, where necessary, kept up to date. The exporter shall take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

Erasure and deletion: For the purposes of Clause 8.5, Section II of Module Two of the Standard Contractual Clauses the data importer shall delete the Customer Data in accordance with paragraph 10 of the DPA.

Audit: The parties acknowledge that the data importer complies with its obligations under Clause 8.9, Section II of Module Two of the Standard Contractual Clauses by (i) acting in accordance with paragraph 11 of the DPA and (ii) exercising its contractual audit rights it has agreed with its subprocessors.

Subprocessors: For the purposes of Clause 9, Section II of Module Two of the Standard Contractual Clauses, the parties agree that option 2: general written authorisation shall apply and the data importer shall notify the data exporter of any changes in accordance with paragraph 8 of the DPA.

Transfer impact assessment: For the purposes of Clause 14(c.), Section III of Module One and Module Two of the Standard Contractual Clauses, the data exporter acknowledges that the data importer may transfer Customer Data to third countries in accordance with this DPA. The data exporter acknowledges the data importer has provided all reasonable information necessary for the data exporter to conclude a transfer impact assessment on or prior to the date of the

Agreement which the data exporter accepts as sufficient to fulfil the data importer's obligations pursuant to Clause 14 of the Standard Contractual Clauses.

For the purposes of Clause 14(c.), 15.1(b) and 15.2, Section III of Module One and Module Two of the Standard Contractual Clauses the parties agree that "best efforts" and the obligations of the data importer under Clause 15.2 shall mean exercising the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a leading practice engaged in a similar type of undertaking under the same or similar circumstances and shall not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

Governing law and Jurisdiction: For the purposes of Clause 17 and 18, Section IV of Module One and Module Two of the EU SCCs, the parties agree that the laws and courts of Ireland will apply. For the purposes of the UK Addendum, the parties acknowledge and accept that the laws and courts of England and Wales will apply.

Annex 1 to the Standard Contractual Clauses

A. LIST OF PARTIES

Data exporter(s)

Name	Customer
Address	As set out in the Agreement
Contact person's name, position and contact details	As set out in the Agreement
Activities relevant to the data transferred under these Clauses	Receipt of the Services
Role (controller/processor)	Controller

Data importer(s)

Name	**Sapia&Co Pty Ltd** (Australia) and / or **Sapia.ai, Inc.** (USA) as applicable to the international transfers being made
Address	As set out in the Agreement
Contact person's name, position and contact details	As set out in the Agreement
Activities relevant to the data transferred under these Clauses	Provider of the Services

Role (controller/processor)	Processor (for the Processing set out at paragraph 2.1). Controller (for the Processing set out at paragraph 2.2 and 2.3)

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Employees or individuals applying for employment with the Customer
Categories of personal data transferred	In the provision of Services to the Customer, the categories of Personal Data we process are Customer Data as defined in the Agreement (including name, phone number and email address), and other Personal Data as defined in the Agreement provided to us directly by the individual applying for employment with you, such as in response to the interview questions asked of the individual during our provision of the Services.
Sensitive data transferred (if applicable)	Dependent on the questions asked by the Customer, but may include personal data about Candidates' age, health, background, and racial or ethnic origin.
The frequency of the transfer	Continuous basis
Nature and purpose(s) of the processing	The processing is carried out to enable us to provide the Services to you during the term of the Agreement, being to: i. collect Candidates' responses to the interview questions you set and your requests for information about Candidates' qualifications and experience to determine a Candidate's suitability for a position; ii. collect Candidates' responses to your questions for your own diversity and inclusion monitoring (if any); and iii. provide you with reports on Candidates' satisfaction with the interview process, their time taken

	to complete each section of the interview and plagiarism rate.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	For the duration of the Agreement
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	The same as applicable to the data importer as described herein

C. COMPETENT SUPERVISORY AUTHORITY

In respect of the EU SCCs, the competent supervisory authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses. In respect of the UK Addendum, the competent supervisory authority shall be read as the Information Commissioner.

Annex 2 to the Standard Contractual Clauses

The data importer shall implement technical and organisational security measures to protect Customer Data as described in paragraph 5 of the DPA.

Part B: UK Addendum

To the extent a restricted transfer of Personal Data is made pursuant to the UK GDPR, this Part B and the following terms shall apply:

Start Date

The UK Addendum is effective from the effective date of the Agreement.

1. **Table 1: Parties**

   Exporter and key contact: As set out in Annex 1 of Part A.

   Importer and key contact: As set out in Annex 1 of Part A.

2. **Table 2: Selected SCCs, Modules and Clauses**

   Modules 1 and 2 of the EU SCCs as incorporated by reference into this DPA including any supplementary clauses set out within this DPA, but not including any other optional clauses unless explicitly specified.

3. **Table 3: Appendix Information**

   As set out in Annex 1 and Annex 2 of the of Part A.

4. **Table 4: Ending this Addendum when the Approved Addendum Changes**

   In the event the Information Commissioner's Office issues a revised Approved Addendum, in accordance with Section 18 of the UK Addendum which as a direct result of such changes has a substantial, disproportionate and demonstrable increase in: (a) the data importer's direct costs of performing its obligations under the Addendum; and/or (b) the data importer's risk under the Addendum, the data importer may terminate this UK Addendum on reasonable written notice to the data exporter in accordance with Table 4 and paragraph 19 of the UK Addendum.