DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated by reference into myInterview's Terms and Conditions at https://www.myinterview.com/terms or other agreement governing the use of myInterview's services ("**Agreement**") entered by and between you, the Customer (as defined in the Agreement) (collectively, "**you**", "**your**", "**Customer**"), and myInterview Ltd. or its Affiliates ("**myInterview**", "**Processor**", "**us**", "**we**", "**our**") to reflect the parties' agreement with regard to the Processing of Personal Data by myInterview solely on behalf of the Customer. Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

Capitalized terms not defined herein shall have the meanings assigned to such terms 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. In the event of any conflict 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.

1. DEFINITIONS

(a) "**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.

(b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which is explicitly permitted to use the Service pursuant to the Agreement between Customer and myInterview but has not signed its own agreement with myInterview and is not a "Customer" as defined under the Agreement.

(c) "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq.

(d) The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR. The terms "**Business**", "**Business Purpose**", "**Consumer**" and "**Service Provider**" shall have the same meaning as in the CCPA.

(e) For the purpose of clarity, within this DPA "**Controller**" shall also mean "**Business**", and "**Processor**" shall also mean "**Service Provider**". In the same manner, Processor's Sub-processor shall also refer to the concept of Service Provider.

(f) "**Applicable Data Protection Laws**" means all privacy and data protection laws and regulations that apply to the Personal Data, including such laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Australia, Israel and the United States of America, if applicable to the Processing of Personal Data under the Agreement including (without limitation) the GDPR, the UK GDPR, the Data Protection Act 2018, the AU Privacy Principles (APPs) of the Privacy Act 1988, and the CCPA, as applicable to the Processing of Personal Data hereunder.

(g) "**Data Subject**" means the identified or identifiable person to whom the Personal Data relates.

(h) “**GDPR**” means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(i) “**Personal Data**” or “**Personal Information**” means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person or Consumer (as defined in the CCPA), which is processed by myInterview solely on behalf of Customer, under this DPA and the Agreement between Customer and myInterview.

(j) “**Services**” means the services provided to Customer by Processor in accordance with the Agreement.

(k) “**Security Documentation**” means the security documentation applicable to the Services purchased by Customer, as updated from time to time and as made reasonably available by myInterview.

(l) “**Sensitive Data**” means Personal Data which includes 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; (e) account passwords; or (f) other information that falls within the definition of “special categories of data” under applicable Data Protection Laws.

(m) “**Sub-processor**” means any third party that Processes Personal Data under the instruction or supervision of myInterview.

(n) “**Standard Contractual Clauses**” means the standard contractual clauses pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (“**SCC**”), which form part of this DPA in the form available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN; each to the extent determined in Section 9.2 of this DPA.

(o) "**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).

(p) “**UK Addendum**” means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses published by the UK Information Commissioner’s Office on March 21, 2022.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties**. The Parties acknowledge and agree that with regard to the Processing of Personal Data performed solely on behalf of Customer, (i) Customer is the Controller of Personal Data, (ii) myInterview is the Processor of such Personal Data, (iii) for the purposes of the CCPA (and to the extent applicable), Customer is the “Business” and myInterview is the "Service Provider" (as such terms are defined in the CCPA), with respect to Processing of Personal Data described in this Section 2.1. The terms "Controller" and "Processor" below hereby signify Customer and myInterview, respectively.

2.2 **Customer's Processing of Personal Data**. Customer, in its use of the Service, and Customer's instructions to the Processor, shall comply with Data Protection Laws. Customer is solely responsible for and shall establish any and all required legal bases in order to collect, Process and transfer to Processor the Personal Data, and to authorize the Processing by Processor, and for Processor's Processing activities on Customer's behalf, including the pursuit of 'business purposes' as defined under the CCPA. Customer is responsible for and warrants that it has provided all the required notices and gained any consents, as may be required by applicable laws, to its data subjects including its employees to allow the lawful processing of Personal Data by Processor.

2.3 **Processor's Processing of Personal Data**. Customer, as the controller of personal data, shall have full control over the means and purposes of the processing tɔhat is carried out as part of the Service. When Processing solely on Customer's behalf under the Agreement, Processor shall Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing for Customer to be able to use the Service; (iii) Processing to comply with Customer's reasonable and documented instructions, where such instructions are consistent with the terms of the Agreement, regarding the manner in which the Processing shall be performed; (iv) rendering Personal Data fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognized by Applicable Data Protection Laws and guidance issued thereunder. The Parties agree that such anonymized data is not considered Customer's Personal Data for the purposes of this Agreement.

2.4 Without derogating from the foregoing in section 2.3, as Processor is subject to regulatory requirements that governs and regulates responsible AI usage, including by mandating developers such as Processor to test its AI powered systems for bias detection and correction, Customer authorizes Processor to use Personal Data for the purpose of complying with legal requirements including by conducting regulatory bias audits.

Processor shall inform Customer without undue delay if, in Processor's opinion, an instruction for the Processing of Personal Data given by Customer infringes applicable Data Protection Laws. To the extent that Processor cannot comply with an instruction from Customer, Processor (i) shall inform Customer, providing relevant details of the issue, (ii) Processor may, without liability to Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) and/or suspend access to the 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, and Customer shall pay to Processor all the amounts owed to Processor or due before the date of termination. Customer will have no further claims against Processor (including, without limitation, requesting refunds for Service) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

2.5 **Details of the Processing**. The subject-matter of Processing of Personal Data by Processor is the performance of the Service pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of Processing) to this DPA.

2.6 **Sensitive Data**. The Parties agree that the Services are not intended for the processing of Sensitive Data, and that if Customer wishes to use the Services to process Sensitive Data, it must first obtain the Processor's explicit prior written consent and Customer is responsible for ensuring any additional conditions that apply to such processing under Applicable Data Protection Laws are fulfilled.

2.7 **CCPA Standard of Care; No Sale of Personal Information**. Processor acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that Processor provides to Customer under the Agreement. Processor shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Customer's behalf, and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it, as stipulated in the Agreement and this DPA. Processor certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any Personal Information Processed hereunder, without Customer's prior written consent, nor taking any action that would cause any transfer of Personal Information to or from Processor under the Agreement or this DPA to qualify as "selling" such Personal Information under the CCPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Requests**. Processor shall, to the extent legally permitted, promptly notify Customer or refer Data Subject or Consumer, as the case may be, to Customer, if Processor receives a request from a Data Subject or Consumer to exercise their rights (to the extent available to them under applicable law) of access, right to rectification, restriction of Processing, erasure ("**right to be forgotten**"), data portability, objection to the Processing, their right not to be subject to automated individual decision making, to opt-out of the sale of Personal Information, or the right not to be discriminated against ("**Data Subject Request**"). Taking into account the nature of the Processing, Processor shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. Processor may refer Data Subject Requests received, and the Data Subjects making them, directly to the Customer for its treatment of such requests.

4. PROCESSOR PERSONNEL

4.1 **Confidentiality**. Processor shall ensure that its personnel engaged in the Processing of Personal Data have committed themselves to confidentiality.

4.2 **Permitted Disclosures**. Without derogating from Section 2.3 above and Section 5 below, Processor may disclose and Process the Personal Data (a) to the extent required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, or (b) otherwise as required by applicable Data Protection Laws (in such a case, Processor shall inform the Customer of the legal requirement before the disclosure, unless legally prohibited from doing so), or (c) on a "need-to-know" basis under an obligation of confidentiality to its legal counsel(s), data protection advisor(s) and accountant(s).

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors**. Customer acknowledges and agrees that (a) Processor's Affiliates may be retained as Sub-processors; and (b) Processor and Processor's Affiliates may each engage third-party Sub-processors in connection with the provision of the Service.

5.2 **List of Current Sub-processors and Notification of New Sub-processors**. The current list of Sub-processors used by Processor to process Personal Data is attached as Schedule 2 to this DPA. Such Sub-processor list includes the identities of those Sub-processors and the entity's country ("**Sub-Processor List**"). The Sub-Processor List as of the date of first use of the Service by Customer is hereby deemed authorized upon first use of the Service.

5.3 **New Sub-processors appointment and Objection Right for New Sub-processors.**

Processor may appoint new Sub Processors and shall give notice of the planned appointment of any new Sub Processor through an email from privacy@myinterview.com. Processor 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 Service. Customer may reasonably object to Processor's use of a new Sub-processor, for reasons relating to the protection of Personal Data intended to be Processed by such Sub-processor, by notifying Processor promptly in writing within seven (7) business days after receipt of Processor's notice of any such intention. Such written objection shall include those reasons for objecting to Processor's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within seven (7) business days following Processor's notice shall be deemed as acceptance of the new Sub-Processor. In the event Customer reasonably objects to a new Sub-processor, as permitted in the preceding sentences, Processor will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Processor is unable to make available such change within thirty (30) days, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Service which cannot be provided by Processor without the use of the objected-to new Sub-processor, by providing written notice to Processor. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Processor. Until a decision is made regarding the new Sub Processor, Processor may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Account. Customer will have no further claims against Processor due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

5.4 **Agreements with Sub-processors**. Processor or a Processor's Affiliate has entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Personal Data. Where Processor engages a new Sub-processor for carrying out specific Processing activities on behalf of the Customer, the same or materially similar data protection obligations as set out in this DPA shall be imposed on such new Sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where the new Sub-processor fails to fulfil its data protection obligations, Processor shall remain fully liable to the Customer for the performance of the new Sub-processor's obligations.

6. SECURITY

6.1 **Controls for the Protection of Personal Data**. Processor shall maintain industry-standard technical and organizational measures for protection of Personal Data Processed hereunder (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data, confidentiality and integrity of Personal Data, including those measures set forth in the Security Documentation), as may be amended from time to time. Upon the Customer's reasonable request, Processor will assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to Processor.

6.2 **Audits and Inspections**. Upon Customer's 14 days prior written request at reasonable intervals (no more than once every 12 months), and subject to strict confidentiality undertakings by Customer,

Processor shall make available to Customer that is not a competitor of Processor (or Customer's independent, reputable, third-party auditor that is not a competitor of Processor and not in conflict with Processor, subject to their confidentiality and non-compete undertakings) all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections, conducted by them (provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Processor's prior written approval. Upon Processor's first request, Customer shall return all records or documentation in Customer's possession or control provided by Processor in the context of the audit and/or the inspection). Customer shall be fully responsible for bearing all the costs and expenses arising from or related to this Section. If and to the extent that the Standard Contractual Clauses apply, nothing in this Section 6.2 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

6.3 In the event of an audit or inspections as set forth above, Customer shall ensure that it (and each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to Processor's premises, equipment, personnel and business while conducting such audit or inspection.

6.4 The audit rights set forth in 6.2 above, shall only apply to the extent that the Agreement does not otherwise provide Customer with audit rights that meet the relevant requirements of Data Protection Laws (including, where applicable, article 28(3)(h) of the GDPR or the UK GDPR).

7. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Processor maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed on behalf of the Customer, including Personal Data transmitted, stored or otherwise Processed by Processor or its Sub-processors of which Processor becomes aware (a "**Data Incident**"). Processor shall make reasonable efforts to identify the cause of such Data Incident and take those steps as Processor deems necessary and reasonable in order to remediate the cause of such a Data Incident to the extent the remediation is within Processor's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users. Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Data Incident which directly or indirectly identifies Processor (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Processor'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 law, Customer shall provide Processor with reasonable prior written notice to provide Processor with the opportunity to object to such disclosure and in any case, Customer will limit the disclosure to the minimum scope required.

8. RETURN AND DELETION OF PERSONAL DATA

Customer can export and delete its data from the Service at any time throughout the subscription term. Without derogating from the above, within 30 days following termination of the Agreement and subject thereto, Processor shall, at the choice of Customer (indicated through the Service or in written notification to Processor), delete all the Personal Data it Processes solely on behalf of the Customer in the manner described in the Agreement, and Processor shall delete existing copies of such Personal Data unless Data Protection Laws require or authorize the storage of the Personal Data. To the extent authorized or required by applicable law, Processor may retain Personal Data solely for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or for compliance with legal obligations. Such Personal Data will be subject to the provisions of this DPA.

9. CROSS-BORDER DATA TRANSFERS

9.1 **Transfers from the EEA, Switzerland and the United Kingdom to countries that offer adequate level or data protection**. Personal Data may be transferred from EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), Switzerland and the United Kingdom ("**UK**") to countries that offer an adequate level of data protection under or 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.

9.2 **Transfers from the EEA, the United Kingdom and Switzerland to other countries.** If the Processing of Personal Data by Processor includes transfers (either directly or via onward transfer) from the EEA ("**EEA Transfer**"), the UK ("**UK Transfer**"), and/or Switzerland ("**Swiss Transfer**") to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliant mechanism as may be adopted by Processor for the lawful transfer of personal data (as defined in the GDPR, the UK GDPR, the FADP, as relevant) outside the EEA the UK or Switzerland, as applicable, then (i) for EEA Transfer, Controller and Processor will enter into the Standard Contractual Clauses Module 2 on Schedule 3; (ii) for UK Transfer, Controller and Processor will enter into the UK Addendum on Schedule 4; (iii) for Swiss Transfer, the terms set forth in Schedule 5 shall apply to any such Swiss Transfer.

Where the transfer of Personal Data is made subject to the Standard Contractual Clauses for EEA Transfer, the "**Data Importer**" thereunder shall be the Processor, and the "**Data Exporter**" shall be the Controller of such Personal Data. Module two will apply when Customer as an Exporter is a controller. Module 3 will apply if Customer as an Exporter is a processor and Processor as an Importer is a sub-processor of the Personal Data being transferred.

In the event of an EEA Transfer or a UK Transfer which relies on the Standard Contractual Clauses or the UK Addendum, the Parties agree to supplement these with the following safeguards and representations, where appropriate:

a. The Processor 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 Controller to the Processor 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 Processor will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the personal data protected under GDPR or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Court ("FISA");

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

- The Processor shall inform the relevant government authority that the Processor is a processor of the Personal Data and that the Controller has not authorized the Processor to disclose the Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to personal data should therefore be notified to or served upon the Controller in writing;

- The Processor will use commercially reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the Processor's control. Notwithstanding the above, (a) the Controller 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 Personal Data, the Processor has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, this subsection shall not apply. In such event, the Processor shall notify the Controller, as soon as possible, following the access by the government authority, and provide the Controller with relevant details of the same, unless and to the extent legally prohibited to do so.

9.3 **Transfers from other countries**. If the Processing of Personal Data by Processor includes transfers (either directly or via onward transfer) from other countries to countries which have not been subject to a relevant Adequacy Decision, Processor ensures any such transfers will be in accordance with the applicable Data Protection Laws.

10. AUTHORIZED AFFILIATES

10.1 **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 Service 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.

10.2 **Communication**. Customer shall remain responsible for coordinating all communication with Processor 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.

11. OTHER PROVISIONS

11.1 **Data Protection Impact Assessment and Prior Consultation**. Upon Customer's reasonable request, Processor shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR or the UK GDPR (as applicable) to carry out a data protection impact assessment related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide, at Customer's cost, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 11.1, to the extent required under the GDPR or the UK GDPR, as applicable.

11.2 **Modifications**. Each Party may by at least forty-five (45) calendar 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) Processor shall make commercially reasonable efforts to accommodate such modification requested by Customer or that Processor believes is necessary; and (b) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Processor to protect the Processor against additional risks, or to indemnify and compensate Processor 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 Processor'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 Processor 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 Processor (including, without limitation, requesting refunds for the Services) pursuant to the termination of the Agreement and the DPA as described in this Section.

MyInterview

Signature:
Name:
Title:
Date:

Customer

Signature:
Name:
Title:
Date:

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Service to Customer. The specific output of the processing is described in the Agreement.

2. Performing the Agreement, this DPA and/or other contracts executed by the Parties;

3. Acting upon Customer's instructions, where such instructions are consistent with the terms of the Agreement;

4. Sharing Personal Data with 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 to facilitate the sharing of Personal Data between the Services and such third-party services);

5. Complying with applicable laws and regulations;

Duration of Processing

Subject to Section 8 of the DPA, Processor will Process Personal Data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Personal Data

As part of the Service, as a data processor on behalf of Customer and in accordance with the Customer's instructions and decisions as to the types of features it utilizes, MyInterview will collect and process the following personal data categories:

- contact details such as name and email address;
- CV (that usually includes information such as work experience, education and skills);
- the position for which candidate is applying.
- A video-based interview of the candidates and their answers to a video-based questionnaire. Customer may request processing of video, images and transcripts derived from such video, either as a raw information or processed for evaluation of the candidate candidacy;
- The Candidates' written responses to questionnaires, including to chats with Taira (Myinterview's AI powered chatting model);
- MyInterview and Customer's evaluations of the candidacy;
- Candidates' personal data collected or created by the Service based on interactions between the candidate, the Customer, and the Service, including video and chatbots interviews evaluations and scores and ratings assigned to the candidate by MyInterview and/or Customer.

Categories of Data Subjects

The Data Subjects whose personal data processed by MyInterview as a Data Processor are Customer's job candidates who use MyInterview's platform.

Schedule 2 - List of Sub-processors

Vendor	Product	Type (Usage)	Location of the data
Amazon AWS	S3 + ECS	Application, Video processing and storage	Based on the client's contract / choice. All data stay in one of the following regions: EU, UK, AU or US
Intercom	Candidates Messaging	Customer support for candidates	EU
Mongo	MongoDB	Database	Based on the client's contract / choice. All data stay in one of the following regions: EU, AU or US
Twilio Inc.	Sendgrid + Twilio SMS	Sendgrid + Twilio SMS, sending SMS and email invites to candidates	U.S. (EU-U.S. Data Privacy Framework certified)
Merge.dev	ATS integrations	Middleware to facilitate the integrations with ATS systems in terms of authentication and data sync	Based on the client's contract / choice. All data stay in one of the following regions: US, EU or APAC
Azure OpenAI	ChatGPT API	Chatbot to interview and score candidates	EU

Schedule 3 – Standard Contractual Clauses

Standard Contractual Clauses (Module 2)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause - OMITTED

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [as indicated in the DPA] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the country where the data exporter is established (in case the data exporter is not established in an EU member state – the courts of Ireland).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such court.

ANNEX I

A. LIST OF PARTIES

The data exporter is the Customer entity named in the Agreement and its contact details are specified in the Agreement.

Activities relevant to the data transferred under these Clauses: the basic processing activities as necessary for Processor to provide the Services as described in the Agreement.

Role (controller/processor): **Controller**

Date: ________________________

Signature: ____________________

The data importer is the Processor entity named in the Agreement and its contact details are specified in the Agreement.

Activities relevant to the data transferred under these Clauses: the basic processing activities as necessary for Processor to provide the Services as described in the Agreement.

Role (controller/processor): **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.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:
The categories of data subjects are described in Schedule 1 (Details of Processing) of this DPA.

Categories of personal data transferred:
The categories of personal data are described in Schedule 1 (Details of Processing) of this DPA.

Sensitive data transferred (if applicable):
The personal data transferred will not concern any special categories of data unless specified in the Agreement.

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

Nature of the processing:
The nature of the processing is described in Schedule 1 (Details of Processing) of this DPA.

Purpose(s) of the data transfer and further processing:
The purpose of the processing is described in Schedule 1 (Details of Processing) of this DPA.

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, unless agreed otherwise in the Agreement and/or the DPA and subject to section 9.2 to the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 is where the data exporter is established. In case the data exporter is not established in an EU member state – the competent supervisory authority of Ireland.

ANNEX II - Technical and Organisational Measures

myInterview implements a comprehensive security framework based on industry best practices and regulatory standards (GDPR, ISO 27001, SOC 2) to ensure the confidentiality, integrity, and availability of personal data. Below are the key technical and organisational security measures in place.

---

1. Measures for Pseudonymisation and Encryption of Personal Data

✓ AES-256 encryption is used for data at rest.

✓ TLS 1.2+ encryption is enforced for data in transit.

✓ Pseudonymisation techniques are used where feasible to protect personally identifiable information (PII) mainly via hashing of the PII or by sending back identifiers instead of PII.

✓ Tokenization is applied to sensitive identifiers to minimize exposure risks (mainly through the use of oAuth).

---

2. Measures for Ensuring Ongoing Confidentiality, Integrity, Availability, and Resilience

✓ Role-Based Access Control (RBAC) restricts data access based on user roles.

✓ Multi-Factor Authentication (MFA) is enforced for all privileged users.

✓ End-to-end logging & monitoring detects unauthorized access attempts.

✓ DDoS protection & network firewalls secure the infrastructure against cyber threats. Intelligent threat detection systems detect any unusual activity.

---

3. Measures for Ensuring Data Recovery & Business Continuity

✓ Automated backups are performed regularly and encrypted at rest (hourly for our Database).

✓ Redundant storage & failover systems ensure high availability.

✓ Disaster recovery plans (DRP) and business continuity plans (BCP) are tested annually.

✓ Recovery time objectives (RTO) & recovery point objectives (RPO) are defined to ensure data restoration in case of incidents (RTO is 8h and RPO is 4h)

---

4. Measures for Regular Testing, Assessment, and Evaluation of Security Controls

✓ Annual third-party penetration testing & vulnerability assessments to identify and mitigate risks.

✓ Continuous security monitoring through automated detection systems.

✓ Regular security audits to ensure compliance with ISO 27001 and SOC 2 standards.

✓ Security Steering Committee reviews security policies quarterly.

---

5. Measures for User Identification and Authorisation

✓ Unique user IDs & authentication mechanisms (SSO, OAuth2, OpenID Connect).

✓ Strict password policies (minimum length, complexity, expiration).

✓ Least privilege principle – users only access the minimum data necessary for their role.

---

6. Measures for the Protection of Data During Transmission

✓ TLS 1.2+ encryption for all external communications.

✓ VPN & encrypted tunnels for remote access.

✓ We use VPCs with the most restrictive permissions for M2M communication

✓ HTTPS enforcement on all web interfaces.

---

7. Measures for the Protection of Data During Storage

✓ AES-256 encryption for stored data.

✓ Access control lists (ACLs) & file permission restrictions.

✓ Cloud storage security (AWS KMS encryption).

✓ Data access logging & real-time security alerts.

---

8. Measures for Physical Security of Data Processing Locations

✓ AWS Data Centers with ISO 27001 & SOC 2 certification ensure secure, monitored facilities.

✓ Restricted access to production environments (only authorized personnel).

✓ CCTV surveillance, biometric access, and 24/7 security monitoring at AWS data centers.

---

9. Measures for Logging, System Configuration, and Security Governance

✓ Detailed logging of system access, user activity, and critical actions.

✓ Regular review of system configurations to enforce secure defaults.

✓ Incident response plans for detecting, mitigating, and reporting security incidents.

---

10. Measures for Compliance, Assurance, and Certification

✓ SOC 2 & ISO 27001 certifications demonstrating adherence to best practices.

✓ Data retention policies ensuring compliance with Data protection laws & contractual obligations.

✓ Annual third-party security audits for process assurance.

---

11. Measures for Data Minimisation, Data Quality, and Limited Data Retention

✓ Data retention policy enforces deletion of personal data after predefined periods.

✓ Automatic anonymization of personal data no longer needed.

✓ Regular data quality assessments to remove redundant or outdated records.

---

12. Measures for Accountability, Data Portability, and Erasure

✓ GDPR-compliant Data Subject Access Request (DSAR) processes.

✓ User consent management & audit trails.

✓ Automated processes for data deletion upon request.

✓ Structured approach for data portability requests in machine-readable formats.

---

13. Measures for Transfers to (Sub-) Processors
For data transfers to sub-processors, myInterview ensures:

✓ Contracts with GDPR-compliant vendors (DPA agreements).

✓ Encryption & secure transfer protocols when sharing data.
✓ Vendor security checks to verify compliance through certifications.
✓ Only necessary data is transferred under strict access controls.

ANNEX III – List of Sub-Processors

The list of Sub-processors is described in Schedule 2 (List of Sub-Processors) of this DPA.

Schedule 4 - UK Addendum

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This UK Addendum forms part of the DPA signed by the parties.
The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The date as of the date the DPA signed by the parties	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	The Customer entity named in the Agreement	MyInterview entity named in the Agreement
Key Contact	As detailed in the Agreement	As detailed in the Agreement
Signature (if required for the purposes of Section 2)	Each party's signature of the DPA shall be considered a signature to the UK Addendum.	Each party's signature of the DPA shall be considered a signature to the UK Addendum.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any):

	Other identifier (if any): Or X the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No	–	–			
2	Yes	Excluded	Excluded	General Authorization	7 days	N/A
3	No	–	–	–	–	
4	No	–	–			–

Table 3: Appendix Information

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

Annex 1A: List of Parties: As indicated in the DPA

Annex 1B: Description of Transfer: As indicated in Annex 1 Details of the Data Processing

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As indicated in Annex II of the SCC.

Annex III: List of Sub processors (Modules 2 and 3 only): As indicated in Annex III of the SCC.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum	Which Parties may end this Addendum as set out in Section 19: ☐ Importer X Exporter ☐ neither Party

changes	

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

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

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

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

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

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

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the

parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

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

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

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

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

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

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

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

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

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

    b. In Clause 2, delete the words:

        > "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses

> pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

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

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit

themselves to the jurisdiction of such courts."; and

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

Amendments to this Addendum

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

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

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

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

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

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

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

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Schedule 5 – Swiss Transfer terms

The Parties agree that the Standard Contractual Clauses as detailed in Schedule 3 of this DPA, shall be adjusted as set out below where the FADP applies to Swiss Transfers:

1. References to the Standard Contractual Clauses mean the Standard Contractual Clauses as amended by Schedule 3;

2. The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for Swiss 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 Swiss Transfers;

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

5. Swiss Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named in Schedule 3;

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 Swiss 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 Swiss Transfers are subject to both the FADP and the GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP insofar as the Swiss Transfers are subject to the FADP;

9. The Standard Contractual Clauses as amended by this Schedule 5 also protect the Personal Data of legal entities until the entry into force of the Revised FADP.