DATA PROCESSING ADDENDUM

This is the Data Processing Addendum ("DPA") referred to in the Terms and Conditions ("Terms and Conditions") entered into between hackajob Ltd. a limited company registered in England under company number 09279930 ("hackajob") and you the Client ("Client"). A copy of the Terms and Conditions can be found here (https://hackajob.com/employer/terms-and-conditions). The Terms and Conditions, together with the Privacy Policy, the Order Forms (in reverse chronological order) and the SLA are hereinafter referred to as the ("Agreement").

All capitalised terms used but not defined herein shall have the meanings ascribed to such terms in the Agreement.

In the course of receiving and using the Services pursuant to the Agreement, the Client will Process hackajob Personal Data (as defined below), and the Parties agree to comply with the terms of this DPA with respect to the Processing (as defined below) of hackajob Personal Data, each acting reasonably and in good faith.

1. DEFINITIONS

"Addendum" means hackajob's International Data Transfer Addendum to the Standard Contractual Clauses, which is attached as Schedule 4 and forms part of this DPA.

"Affiliate" means an entity which controls, is controlled by, or is under common control with, a party, and control means the ability to vote 50% or more of the voting securities of any entity or otherwise having the ability to influence and direct the polices and direction of an entity;

The terms, "Commission", "Controller", "Data Subject", "Data Protection Impact Assessment", "Member State", "Personal Data", "Personal Data Breach", "Processing", "Processor", and "Supervisory Authority" shall have the same meaning as in the GDPR and UK GDPR (as appropriate), and their cognate terms shall be construed accordingly.

"Data Privacy Law" means, as applicable, EU Data Protection Laws and UK Data Protection Laws and the data protection laws applicable in the USA from time to time, including without prejudice to the foregoing, the California Consumer Privacy Act 2018 and the California Privacy Rights Act 2020, the Virginia Consumer Data Protection Act 2021 and the Colorado Privacy Act 2021 and all other applicable, national, federal, state and other laws, rules and regulations relating to the Processing of Personal Data and data privacy or data protection that may exist in any relevant jurisdiction.

"EU Data Protection Laws" means (i) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (ii) the GDPR in each case, as may be amended, superseded or replaced and all applicable laws and regulations relating to the processing of personal data and privacy in the European Union including where applicable the guidance and codes of practice issued by the relevant Supervisory Authority;

"European Data" means hackajob Personal Data that is subject to the protection of EU Data Protection Laws.

"GDPR" means the EU General Data Protection Regulation 2016/679.

“hackajob Personal Data” means all Personal Data Processed by the Client or its Sub-processors on behalf of hackajob pursuant to or in connection with the Agreement.

“Thena Personal data” means all Personal Data Processed by hackajob (as Processor) on behalf of the Client (as Controller) in connection with the Thena Services, as further described in Schedule 5 (Thena Processing Details).

“Permitted Purpose” means, in respect of each party, fulfilling its obligations under the Agreement.

“Standard Contractual Clauses” means the standard contractual clauses issued by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any set of clauses approved by the European Commission or a Supervisory Authority which subsequently amends, replaces or supersedes the same which standard contractual clauses are attached as Schedule 3 and forming part of this DPA.

“Sub-processor” means any person or legal entity (including any third party and any Affiliate of the Client, but excluding an employee of the Client or any of its Sub-processors) appointed by or on behalf of the Client or any of its Affiliates to Process hackajob Personal Data.

“UK Data” means hackajob Personal Data that is subject to the protection of UK Data Protection Laws.

“UK Data Protection Laws” means the Data Protection Act 2018, the retained European Union law version of the GDPR (the “UK 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, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and all applicable laws and regulations relating to the processing of personal data and privacy in the United Kingdom including where applicable the guidance and codes of practice issued by the relevant Supervisory Authority;

“USA” means the United States of America;

2. PROCESSING OF PERSONAL DATA (Controller → Processor and Processor → Controller)

2.1 Details of the Processing. The Parties acknowledge and agree that with regard to the Processing of hackajob Personal Data, hackajob is the Controller, the Client is the Processor and that the Client may engage Sub-processors to Process hackajob Personal Data on its, and ultimately the Controller’s, behalf subject to the requirements set out in Clause 5 (Sub-processors) below. For certain Services within the hackajob Product Suite (including *Thena*), the roles of the Parties are reversed: the Client acts as the Controller and hackajob acts as the Processor. The applicable processing details for such Services are set out in Schedule 5 (Thena Processing Details).The subject matter, duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (*hackajob Personal Data Processing Details*) to this DPA which forms part of this DPA.

2.2 hackajob's Processing of Personal Data. hackajob shall process Personal Data pursuant to the Agreement, including through its engagement of the Client as Processor, in accordance with the requirements of Data Privacy Law. For the avoidance of doubt, hackajob's instructions for the Processing of hackajob Personal Data shall comply with Data Privacy Law. This DPA and the Agreement are, at the time of signature of the Agreement, hackajob's documented instructions to the Client for the Processing of hackajob Personal Data. Any additional or alternate instructions must be agreed upon and documented in writing separately (which may be by email).

2.3 The Client's Processing of hackajob Personal Data. The Client shall treat hackajob Personal Data as Confidential Information and shall only Process hackajob Personal Data on behalf of hackajob and in accordance with hackajob's documented instructions, including with regard to transfers of hackajob Personal Data outside of the USA for the following purposes: (i) Processing in accordance with the Agreement; and (ii) Processing to comply with other documented reasonable instructions provided by hackajob (e.g., via email) where such instructions are consistent with the terms of the Agreement. The Client will Process hackajob Personal Data in compliance with Data Privacy Law. hackajob hereby warrants, represents, and undertakes that the hackajob Personal Data shall comply with Data Privacy Law in all respects including, but not limited to, its collection, holding, and Processing.

2.4 General. Taking into account the nature of the Processing of hackajob Personal Data and information available to the Client, subject to the specific provisions of this DPA, the Client shall assist hackajob (at the Client's reasonable expense, where such assistance exceeds standard Data Subject Requests (as hereinafter defined) response assistance) in its efforts to comply with its obligations under Data Privacy Law, including obligations relating to responding to Data Subject Requests, and in ensuring compliance with its obligations with respect to records of processing, security of Processing, notifications of Personal Data Breaches to Data Subjects and Supervisory Authorities, Data Protection Impact Assessments, and consultations with Supervisory Authorities. The Client shall (at hackajob's reasonable expense), make available to hackajob all information, to the extent the Client is in possession of such information, necessary for hackajob, as Controller, to meet its obligations under Data Privacy Law, and allow for and contribute to audits, including inspections, conducted by hackajob or another auditor mandated by hackajob in all cases subject to and in the manner provided for in Clause 6 (Security) below.

2.5 Client Records of Processing. The Client shall maintain a written record of all categories of processing activities carried out on behalf of hackajob including:

(a) its own name and contact details, the name and contact details of hackajob (and its Affiliates), any other processors and, where applicable, the data protection officer;

(b) the categories of processing activities performed on behalf of hackajob; and

(c) Details of any transfers of hackajob Personal Data outside the European Union or European Economic Area including:

(i) The identification of the third country.

(ii) Where applicable, documentation of suitable safeguards in accordance with Article 49(1) of the General Data Protection Regulation.

3. CLIENT PERSONNEL

3.1 Confidentiality. The Client shall ensure that its personnel engaged in the Processing of hackajob Personal Data have the appropriate background and experience, are informed of the confidential nature of the hackajob Personal Data, have received appropriate training on their responsibilities and have either executed written confidentiality agreements committing them to holding the hackajob Personal Data in confidence or are under an appropriate statutory obligation of confidentiality. The Client shall ensure that such confidentiality obligations survive the termination of the personnel engagement. These Confidentiality provisions are supplementary to (and do not replace) the Confidentiality provisions in the Agreement.

3.2 Reliability. The Client shall take commercially reasonable steps to ensure the reliability of any the Client personnel engaged in the Processing of, or that has access to, hackajob Personal Data.

3.3 Limitation of Access. The Client shall ensure that its employees' access to hackajob Personal Data is strictly limited to those personnel requiring such access to perform the Services in accordance with the Agreement.

4. DATA SUBJECT REQUESTS

4.1 Data Subject Requests. Taking into account the nature of the Processing, the Client shall assist hackajob by providing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of hackajob's obligation to respond to requests from Data Subjects to exercise their rights under applicable Data Privacy Law ("Data Subject Requests"). The Client agress to:

(a) Provide hackajob with any requested information or assistance necessary to respond to a Data Subject Request within ten (10) business days of hackajob's written request, unless otherwise mandated by applicable law.

(b) Notify hackajob promptly, and in any case within five (5) business days, if the Client directly receives a Data Subject Request. The Client shall not respond to any such request without hackajob's prior written instructions.

(c) Ensure that all necessary technical and organisational measures are in place to facilitate hackajob's ability to respond to Data Subject Requests in a timely manner, including the ability to locate, retrieve, and, if applicable, delete hackajob Personal Data as required.

5. SUB-PROCESSORS

5.1 Use of Sub-processors.

(a) Both Parties acknowledge and agree that:

(i) hackajob may engage third-party Sub-processors for the fulfilment of its obligations under the Agreement and the Processing of personal data, including hackajob Personal Data. Such Sub-processors are listed in Annex 1, which will be updated by Hackajob from time to time as necessary.

(ii) The Client's Affiliates may be retained as Sub-processors; and

(iii) The Client may engage third-party Sub-processors for the fulfilment of its obligations under the Agreement and related Processing of hackajob Personal Data, all in accordance with Standard Contractual Clause 9 below and as follows:

(b) The Client agrees that:

(i) The Client will restrict the Sub-processor's access to hackajob Personal Data only to what is necessary under the Agreement, and the Client will prohibit the Sub-processor from accessing hackajob Personal Data for any other purpose.

(ii) The Client will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor is performing the same Processing services that are being provided by the Client under this DPA, the Client will impose on the Sub-processor the same standard of contractual obligations that the Client has under this DPA.

(iii) The Client will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause the Client to breach any of the Client's obligations under this DPA.

5.2 Notification of New Sub-processors. hackajob may engage third-party Sub-Processors to assist in the Processing of hackajob Personal Data as necessary to provide the Services. A list of current Sub-Processors is included in Annex 1 to this DPA, and hackajob will maintain and update this list as necessary. hackajob shall notify the Client of any intended additions, removals, or replacements of Sub-Processors at least thirty (30) calendar days in advance of the change taking effect. This notification may be provided via email, through the Client portal (if applicable), or by updating a publicly accessible webpage that contains the current Sub-Processor list. Clients may review the updated Sub-Processor list and, within ten (10) business days of receiving notice of any changes, raise any reasonable and documented concerns regarding a new Sub-Processor's ability to meet the data protection requirements set forth in this DPA. hackajob shall, in good faith, address such concerns by providing additional information about the safeguards in place with the Sub-Processor or by taking other reasonable steps to address the Client's concerns. hackajob warrants that any Sub-Processor it engages will be bound by written agreements imposing data protection obligations no less protective than those set forth in this DPA and in compliance with applicable Data Privacy Laws, including GDPR.

6. SECURITY

6.1 Controls for the Protection of hackajob Personal Data. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Client shall maintain appropriate technical and organisational measures for protection of the security (including protection against Personal Data Breach), confidentiality and integrity of hackajob Personal Data, including (without limitation) those measures set out in

Article 32 of the GDPR, and as described in Schedule 2 to this DPA (*Security Measures*) ("Security Measures"). Notwithstanding any provision to the contrary, the Client may modify or update the Security Measures at its discretion provided that such modification or update does not result in any degradation in the protection offered by the Security Measures and provided those Security Measures comply with Data Privacy Law. The Client shall regularly monitor compliance with such measures. In assessing the appropriate level of security, the Client shall take account of the risks that are presented by Processing, in particular from a Personal Data Breach.

6.2 Third Party Certifications. Upon hackajob's written request at reasonable intervals (as provided below), and subject to the confidentiality obligations set forth in the Agreement, the Client shall allow for and contribute to audits and inspections ("Audits") conducted by hackajob (or hackajob's independent, third-party auditor that is subject to confidentiality obligations at least as restrictive as those set out in the Agreement) by providing any information reasonably necessary to demonstrate the Client's compliance with the obligations set forth in this DPA, including without limitation in the form of a copy of the Client's then most recent third-party audits or certifications, as applicable, that the Client makes available to its clients generally, or such other information as hackajob may reasonably request.

6.3 Right to Audit. The Client shall maintain complete and accurate records and information to demonstrate its compliance with this DPA, and hackajob (or its permitted third-party auditor as provided above) may perform an Audit remotely or on-site, up to one (1) time per year, with at least three (3) weeks' advance written notice, unless hackajob knows or reasonably suspects the Client has suffered a Personal Data Breach or as otherwise required by hackajob's regulators or Applicable Law. If hackajob requests an on-site Audit, the following terms shall apply: (a) such Audit shall be limited to facilities operated by the Client and shall not exceed two (2) business days; (b) before the commencement of any such on-site Audit, hackajob and the Client acting in good faith shall mutually agree upon the scope and timing of, and procedures relating to, the Audit with a view towards minimising the disruption of the Client's business; and (c) hackajob shall promptly notify the Client with reasonably detailed information regarding any non-compliance discovered during the course of an Audit. The material and Data audited will only be those relating specifically to the subject matter of this Agreement.

6.4 Audits Pursuant to Standard Contractual Clauses. The Parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Clauses 6.2 and 6.3 above.

6.5 Personal Data Breaches. The Client will notify hackajob without undue delay and in any case within forty-eight (48) hours after it becomes aware of any Personal Data Breach and shall provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by hackajob. The notification shall at least:

(a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of hackajob Personal Data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

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

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

6.6 At hackajob's request, the Client will promptly provide hackajob with such reasonable assistance as necessary to enable hackajob to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if and to the extent hackajob is required to do so under Data Privacy Law.

7. DATA TRANSFERS

Transfer of hackajob Personal Data to the Client. The Parties acknowledge that in connection with the performance of its obligations under the Agreement, the Client and hackajob may each be a recipient of Personal Data subject to Data Privacy Law. In relation to hackajob Personal Data, the Client will be a data importer or exporter as applicable, and in relation to Thena Personal Data (and any Other product-specific data described in a Schedule where hackajob acts as Processor), hackajob acts as the data importer under the Standard Contractual Clauses (Module2: Controller → Processor), and where relevant, the UK International Data Transfer Addendum. The Parties agree that (1) in relation to hackajob European Data hackajob will process such data in compliance with the Standard Contractual Clauses and, in relation to hackajob UK Data, in compliance with the UK Addendum (2) in relation any Personal Data Processed by hackajob as processor (including Thena Personal Data and any future Product-specific data described in an applicable Schedule), the same transfer safeguards, namely the EU Standard Contractual Clauses (Module 2 – Controller → Processor) and the UK International Data Transfer Addendum shall apply. (3)iIf and to the extent either the Standard Contractual Clauses or the UK Addendum conflict with any provision of this DPA, those instrumentsshall prevail to the extent of such conflict.

If there is any conflict between the terms of the Agreement and this DPA, then (unless expressed otherwise herein) the Terms of the DPA shall prevail to the extent of such conflict.

8. INDEMNITY

8.1 Neither Party shall be liable for indirect, consequential, or incidental damages, including lost profits or business interruption, except in cases of gross negligence, fraud, or willful misconduct.

9. TERMINATION

9.1 The term of this DPA will end simultaneously and automatically at the later of (i) the date of expiration or termination of the Agreement and (ii) the first date when all hackajob Personal Data Processed by either Party under this DPA (including any Product-specific Personal Data described in the applicable Schedules) has been delted or returned in accordance with its terms. After the termination of this DPA, the Client will delete or return all hackajob Personal Data (including copies thereof) promptly upon its receipt of written notice from hackajob specifying whether it chooses for such hackajob Personal Data to be deleted or returned, save that this requirement shall not apply to the extent the Client is required Laws to retain some or all of hackajob Personal Data. Concerning European Data, Laws as used in this clause is limited to EU Data Protection Laws.

10. GENERAL

10.1 This DPA may only be amended with the written consent of both Parties.

10.2 The Parties to this DPA hereby submit to the choice of law and jurisdiction stipulated in the Agreement with respect to any disputes or claims that arise under this DPA, subject to the Standard Contractual Clauses.

SCHEDULE 1

HACKAJOB PERSONAL DATA PROCESSING DETAILS

Categories of data subjects whose personal data is transferred

Candidates and Clients

Categories of personal data transferred:

- For Candidates we capture the following data fields:
  - Full Name
  - Phone Number
  - Address and Location
  - Email Address
  - Work and Education History
  - Desired Job Positions and Locations
  - Desired Salary
  - Industry Preferences
  - Company Size Preferences
  - Qualifications
  - Visa Status
  - References
  - Profile Photo

- For Clients (users of the platform) we capture the following data fields:
  - Full Name
  - Phone Number
  - Work Email Address

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Medical conditions and health data contained in CVs/Resumés, gender, ethnicity, neurodiversity, sexual orientation.

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

Continuous

Nature of the processing:

The processing of Personal Data involves the collection, storage, transmission, and use of data as necessary to provide and facilitate the Services, including enabling communication and data exchange between Candidates and Clients, ensuring compliance with documented instructions provided by hackajob, fulfilling contractual obligations, and resolving disputes related to the Agreement.

Purpose(s) of the data transfer and further processing

To assess the suitability of and the Engagement of Candidates

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

As between the Client and hackajob the duration of the Processing under this DPA is determined by hackajob; provided that, generally the duration of the Processing of hackajob Personal Data by the Client shall be for the Term and for the duration of the Agreement.

SCHEDULE 2

SECURITY MEASURES

The Client will adopt industry-standard security practices and policies to ensure the protection of Personal Data and prevent security incidents. These measures include:

1. Administrative Safeguards
   - Policies and procedures for acceptable use, access control, disciplinary action, and data minimization.
   - Security awareness training for personnel handling Personal Data.
2. Technical Safeguards
   - Secure transfer of Personal Data using SSL encryption.
   - Password protection and multi-factor authentication.
   - Regular system monitoring, dashboards, and alerts for enhanced control.
   - Implementation of secure development practices for applications.
3. Physical Safeguards
   - Physical access controls to secure facilities and data storage.
   - Procedures for secure disposal of sensitive data and equipment.
4. Risk and Incident Management
   - Regular risk assessments and vulnerability management.
   - Penetration testing and patch management to address system vulnerabilities.
   - Incident response plan to detect, respond to, and recover from Data Breaches.
5. Third-Party Management
   - Written agreements with third-party Data Processors and Sub-Processors to ensure compliance with data protection standards.

By adhering to these measures, the Client ensures the security and integrity of hackajob's Personal Data in line with industry best practices.

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

These Clauses apply whether hackajob acts as data exporter or data importer, as described in Clause 2 and the applicable Schedule

hackajob, as defined in the Agreement (the "data exporter")

and

The Client, as defined in the Agreement (the "data importer")

each a 'party'; together 'the parties',

HAVE AGREED that the Standard Contractual Clauses shall apply in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

The Standard Contractual Clauses shall be applied as follows:

STANDARD CONTRACTUAL CLAUSES

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, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679.

(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 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(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 the 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

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

<u>SECTION II – OBLIGATIONS OF THE PARTIES</u>

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.

MODULE TWO: Transfer controller to processor

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[1] (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.

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Clause 9

Use of sub-processors for Cross-Border Transfers

MODULE TWO: Transfer controller to processor

(a) hackajob, as data exporter, may engage third party subprocessors to process personal data on its behalf in accordance with this DPA. The obligations regarding subprocessors outlined in Section 5 of the DPA apply to all subprocessors engaged for cross-border data transfers.

(b) hackajob shall ensure that any Subprocessor involved in a transfer of hackajob Personal Data outside the European Economic Area (EEA) or the UK is bound by:

- Standard Contractual Clauses (SCCs) as adopted by the European Commission or UK Addendum; or
- Other lawful mechanisms under applicable Data Privacy Laws (e.g., adequacy decisions or binding corporate rules).

(c) hackajob remains fully responsible for any Processing performed by subprocessors engaged for cross-border data transfers and warrants that all such subprocessors comply with the requirements of this DPA and applicable Data Privacy Laws.

(d) The list of current subprocessors, including their locations and the type of Processing they perform, is maintained in Annex 1. hackajob will notify the Client of changes to this list in accordance with Section 5 of the DPA.

(e) Where necessary to demonstrate compliance with applicable Data Privacy Laws, hackajob shall, upon request, provide the Client with a copy of the relevant transfer mechanism (e.g., executed SCCs) or a summary of the safeguards in place with its subprocessors.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(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.

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(a) 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.

(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

MODULE TWO: Transfer controller to processor

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(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[2];

(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

[2] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

MODULE TWO: Transfer controller to processor

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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 minimisation

(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

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which hackajob is established. If hackajob does not have an EU establishment, the governing law shall be the law of an EU Member State chosen by hackajob.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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

(f) 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.

(g) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. Name: hackajob Ltd. company number 09279930

Address: 3rd Floor 1 Ashley Road, Altrincham, Cheshire, United Kingdom, WA14 2DT

Contact person's name, position and contact details: Pete Bulley, COO, pete@hackajob.co

Activities relevant to the data transferred under these Clauses:

- Collecting, storing, and managing personal data of Candidates and Clients to facilitate recruitment and hirings services.
- Sharing Candidate profiles and associated data with Clients to assess the suitability of Candidates for potential roles.
- Ensuring compliance with applicable data protection laws (e.g., GDPR, UK GDPR) when managing and transferring personal data to the Data Importer.

Role (controller/processor): Controller

DPO: Scott Simpson, dpo@hackajob.co

EU hackajob representative: hackajob Ltd Londra Sucursala Iasi, Solomons building, 37 Sf Lazar Street, 700049, Iasi, Romania

Data importer(s): The Client as defined in the Agreement with details as specified in the Order Form under the Agreement.

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

- Storing, organising, and managing hackajob Personal Data to facilitate recruitment-related services
- analysing and evaluating Candidates profiles, qualifications, and suitability for potential roles
- facilitating communication between hackajob and the Client for recruitment purposes

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Candidates and Clients

Categories of personal data transferred:

- For Candidates we capture the following data fields:
  - Full Name
  - Phone Number
  - Address and Location
  - Email Address
  - Work and Education History
  - Desired Job Positions and Locations
  - Desired Salary
  - Industry Preferences
  - Company Size Preferences
  - Qualifications
  - Visa Status
  - References
  - Profile Photo

- For Clients (users of the platform) we capture the following data fields:
  - Full Name
  - Phone Number
  - Work Email Address

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Medical conditions and health data contained in CVs/Resumés, gender, ethnicity, neurodiversity, sexual orientation.

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

Continuous

Nature of the processing:

The processing of Personal Data involves the collection, storage, transmission, and use of data as necessary to provide and facilitate the Services, including enabling communication and data exchange between Candidates and Clients, ensuring compliance with documented instructions provided by hackajob, fulfilling contractual obligations, and resolving disputes related to the Agreement.

Purpose(s) of the data transfer and further processing

To assess the suitability of and the Engagement of Candidates

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

As between the Client and hackajob the duration of the Processing under this DPA is determined by hackajob; provided that, generally the duration of the Processing of hackajob Personal Data by the Client shall be for the Term and for the duration of the Agreement.

Purpose of data transfers to (sub-) processors:

The purpose of transferring personal data to subprocessors is to enable hackajob to deliver and facilitate the Services as outlined in the Agreement. Subprocessors are engaged to perform specific, technical, and operational activities that support the functionality, security, and delivery of the Services.

A current list of Sub-Processors engaged by hackajob in connection with the provision of its products and services (the *hackajob Product Suite*) is available at: https://docs.google.com/document/d/1EE-1M3tWXm9wLY7xUMpeEmxD_DKYuZdcBJN49iqEv70/edit?tab=t.0

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

hackajob Ltd Londra Sucursala Iasi, Solomons building, 37 Sfantul Lazar street, 700049, Iasi, Romania

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Schedule 2 above and in addition:

MODULE TWO: Transfer controller to processor

This annex describes the technical and organisational measures implemented by the Data Importer (Client and any engaged subprocessors) to ensure an appropriate level of security for hackajob Personal Data. These measures are designed to safeguard the confidentiality, integrity, and availability of personal data, considering the nature, scope, and risks associated with processing.

- 1. Administrative Safeguards
    - 1.1 Security Policies and Governance

- The Data Importer implements documented security policies and procedures governing data protection, access controls, and security monitoring.
- Security measures comply with ISO 27001, SOC 2 Type II, GDPR, and other applicable data protection standards.

- Security policies cover:
    - Access control and user authentication
    - Data minimisation and storage limitations
    - Incident response and breach notification procedures
    - Regular security audits and compliance monitoring

1.2 Security Awareness and Training

- Personnel handling hackajob Personal Data receive regular security awareness training, including:
    - Recognising phishing and social engineering attacks
    - Secure password management and authentication best practices
    - Incident handling and data breach response protocols

2. Technical Safeguards

2.1 Data Encryption and Pseudonymisation

- All personal data at rest is encrypted using industry-standard encryption (e.g., AES-256).
- All personal data in transit is protected with TLS 1.2 or higher encryption.
- Pseudonymisation techniques are applied where feasible to minimise data exposure in case of a breach.

2.2 Access Control and Authentication

- Access to hackajob Personal Data is strictly limited based on the principle of least privilege (PoLP).
- Role-Based Access Control (RBAC) ensures that only authorised users can access personal data.
- Multi-Factor Authentication (MFA) is enforced for all access to systems containing personal data.
- Access logs are continuously monitored to detect and prevent unauthorised access.

2.3 Secure System Development and Maintenance

- Secure coding practices, including regular security testing, are applied in software and system development.
- Security vulnerabilities are identified and patched within defined SLAs to minimise risk exposure.
- Systems undergo regular penetration testing and security assessments.

3. Physical Security Measures

3.1 Secure Data Centers and Infrastructure

- Personal data is stored in secure, access-controlled environments with:
    - 24/7 physical security and surveillance
    - Biometric authentication and restricted access for authorised personnel only
    - Redundant power and failover systems to prevent data loss

    - 3.2 Device and Endpoint Security

  - All devices used to access hackajob Personal Data are secured with:
    - Full disk encryption and endpoint security solutions
    - Automatic locking and remote wipe capabilities in case of theft or compromise
    - Secure disposal procedures for data-bearing equipment

- 4. Risk and Incident Management

    - 4.1 Continuous Monitoring and Threat Detection

  - Automated monitoring and intrusion detection systems identify suspicious activities.
  - Security logs are stored and reviewed to detect potential threats.
  - Alerts and security dashboards provide real-time visibility into security events.

    - 4.2 Incident Response and Breach Notification

  - A formal incident response plan (IRP) is in place to:
    - Detect and contain security incidents
    - Assess and mitigate the impact on personal data
    - Notify hackajob within 72 hours of a confirmed data breach affecting Hackajob Personal Data.
  - Security incidents and breaches are logged, investigated, and reported to ensure continuous improvement.

- 5. Subprocessor and Third-Party Management

    - 5.1 Subprocessor Due Diligence and Security Standards

  - The Data Importer ensures that all subprocessors and vendors processing hackajob Personal Data:
    - Sign a Data Processing Agreement (DPA) that enforces GDPR-compliant security measures.
    - Implement security policies and controls equivalent to those outlined in this Annex.
    - Undergo regular audits and risk assessments to validate compliance.

    - 5.2 Secure Data Transfers

  - Personal data is only transferred to subprocessors with:
    - Standard Contractual Clauses (SCCs) or an adequacy decision
    - Documented technical and organisational safeguards
    - Encryption and access restrictions to prevent unauthorised access

- 6. Data Retention and Secure Erasure

    - 6.1 Data Retention Policy

  - Personal data is retained only for the duration necessary for the purpose of processing.

    - Retention schedules align with contractual and legal obligations to ensure compliance.

        - 6.2 Secure Data Deletion

    - Upon contract termination, personal data is:
        - Permanently deleted within 30 days
        - Securely erased from backups, unless legally required to retain for compliance
        - Certified as deleted upon request to confirm data removal

- 7. Compliance and Security Testing

    - The Data Importer implements regular security audits and testing to ensure continuous compliance with:
        - ISO 27001, SOC 2 Type II, GDPR, and other regulatory frameworks
        - Independent third-party security assessments to validate controls
        - Continuous improvement processes to enhance data protection

SCHEDULE 4

HACKAJOB ADDENDUM

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Scope of Transfers.
This Addendum applies to all Restricted Transfers of Personal Data under the Agreement. Depending on the particular Service:

- For *Source* (and any Service where hackajob acts as Controller), hackajob is the data **exporter** and the Client is the data **importer**.

- For *Thena* (and any Service where hackajob acts as Processor), the **Client** is the data **exporter** and **hackajob** is the data **importer**.
  The Parties agree that the EU Standard Contractual Clauses and this UK Addendum shall apply in either case, with the roles adjusted accordingly.

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

This is the International Data Transfer Addendum ("Addendum") referred to in hackajob's Client Terms and Conditions ("Terms") which are available to view here: https://hackajob.com/employer/terms-and-conditions

Unless specified otherwise, words and phrases used in this Addendum shall have the meanings as described to them in the Terms.

Part 1: Tables

Table 1: Parties

Start date	The Date of commencement of delivery of Services in accordance with the relevant Order Form.	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	hackajob Ltd. a limited company registered in England under company number 09279930 with its registered address at 3rd Floor 1 Ashley Road, Altrincham, Cheshire, United Kingdom, WA14 2DT;	The Client named in the Order Form;
Key Contact	As specified in the Order Form;	As specified in the Order Form;
Signature (if required for the purposes of Section 2)	Not Required. This Addendum is deemed to be entered into when the parties enter into the Agreement	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	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?

2	2	2	2	2	2	YES

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: Annex 1A to the Standard Contractual Clauses

Annex 1B: Description of Transfer: Annex 1B to the Standard Contractual Clauses.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II to the Standard Contractual Clauses.

Annex III: List of Sub processors (Modules 2 and 3 only): Not Applicable.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: The Parties can end the Addendum before the end of the Subscription Term in accordance with the termination provisions contained in the Terms.

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.

SCHEDULE 5
Thena Processing Details (Controller → Processor)

1. Subject Matter and Purpose

The subject matter of the processing is applicant data provided by the Client via its Applicant Tracking System (ATS).
The purpose is to enable the Client to screen, filter, and rank applicants using Thena's AI-powered functionality, to assist in recruitment decision-making.

2. Duration

Processing continues for the duration of the Agreement and any subsequent data retention period permitted under clause 9 of the DPA, following which all personal data shall be deleted or returned to the Client within thirty (30) days, unless retention is required by law.

3. Nature of Processing

Collection, analysis, scoring, and ranking of applicant data; generation of AI-powered insights and reports; storage of relevant data to facilitate the Client's ongoing recruitment activities.

4. Categories of Data Subjects

Applicants whose personal data has been lawfully collected and transferred to Thena by the Client.

5. Types of Personal Data

Full name, contact details (email address, telephone number), location, CV/resumé content (employment and education history, skills, qualifications), responses to application questions, and other data fields provided by the Client.

6. Sensitive Data

Thena is not designed to process special-category data. Should such data be submitted, it will be processed only under the Client's explicit written instruction and subject to appropriate safeguards.

7. Processor Obligations

hackajob shall:

- Process Personal Data solely on the Client's documented instructions and in compliance with Data Protection Legislation;

- Ensure that only authorised personnel with appropriate confidentiality obligations have access to Personal Data;

- Maintain up-to-date records of processing activities carried out on behalf of the Client;

- Notify the Client within forty-eight (48) hours of becoming aware of a Personal Data Breach;
- Implement appropriate technical and organisational security measures as set out in **Schedule C (Security Measures)**;
- Assist the Client in responding to data subject requests and fulfilling its obligations under Articles 32–36 GDPR (including DPIAs and breach notifications);
- Make available all information reasonably necessary to demonstrate compliance and allow for audits as described in clause 6 of the DPA.

8. Sub-Processors
hackajob may engage third-party Sub-Processors to assist in providing the Thena Services.

- A current list of Sub-Processors is maintained by hackajob and available upon written request.
- hackajob shall provide not less than thirty (30) days' written notice of any intended changes.
- hackajob remains fully liable for any act or omission of its Sub-Processors that causes a breach of this DPA.

9. Cross-Border Data Transfers
Where Personal Data is transferred outside the UK or EEA, the Parties agree to rely on the EU Commission Standard Contractual Clauses (Module 2: Controller to Processor) and the UK International Data Transfer Addendum, both of which are incorporated by reference.

10. Security
hackajob shall implement industry-standard technical and organisational security measures, including encryption in transit and at rest, multi-factor authentication, access controls, regular penetration testing, and staff data protection training. Details are set out in Schedule C.

11. Data Subject Rights
hackajob shall promptly notify the Client if it receives a request from a data subject and shall not respond directly unless authorised in writing. hackajob shall provide all reasonable assistance to enable the Client to respond to such requests within the time limits prescribed by law.

12. Audit Rights
Upon written request and with reasonable notice, the Client may audit hackajob's compliance with this Schedule. hackajob may satisfy audit requests by providing up-to-date independent

audit reports (such as ISO 27001 or SOC 2 Type II certifications) or similar evidence of compliance.

13. Return or Deletion of Data

Upon termination or expiry of the Agreement, hackajob shall, at the Client's election, securely delete or return all Personal Data and certify such deletion, save to the extent retention is required by Applicable Law.

14. Liability

Each Party's liability under this Schedule shall be governed by the limitation of liability provisions contained in the DPA and the Agreement.