

DATA PROCESSING ANNEX

CONTENTS

CLAUSE

1.	Definitions and Interpretation	1
2.	Personal data types and processing purposes	2
3.	hackajob's obligations	2
4.	hackajob's employees	3
5.	Security	3
6.	Personal data breach	3
7.	Cross-border transfers of personal data	4
8.	Subcontractors	4
9.	Complaints, data subject requests and third-party rights	5
10.	Term	5
11.	Data return and destruction	5
12.	Records	6
13.	Audit	6
14.	Warranties	6
15.	Notice	7

This Personal Data Processing Annex (**Annex**) sets out the additional terms, requirements and conditions on which hackajob will process Personal Data when providing Services under its Terms of Use (**Terms**). This Annex contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors.

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

- 1 Business Purposes:** the services to be provided by us as set out in the Terms and Part A to this Annex.
- 2 Commissioner:** the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).
- 3 Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing:** have the meanings given to them in the Data Protection Legislation.
- 4 Data Protection Legislation:** all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party.
- 5 Data Subject:** the identified or identifiable living individual to whom the Personal Data relates.
- 6 EEA:** the European Economic Area.
- 7 Personal Data:** means any information relating to an identified or identifiable living individual that is processed by hackajob on your behalf as a result of, or in connection with, the provision of the services under the Terms an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- 8 Processing, processes, processed, process:** any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.
- 9 Personal Data Breach:** a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.
- 10 Records:** has the meaning given to it in Clause 12.
- 11 Term:** this Agreement's term as defined in Clause 10.
- 12 UK GDPR:** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.
- 13 User:** any client of hackajob Limited

1.2 This Annex is subject to the terms of the Terms and is incorporated into the Terms.

2. Personal data types and processing purposes

2.1 For the purpose of the Data Protection Legislation:

- (a) hackajob is the Data Controller and retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the User.
- (b) The User is the Data Processor

3. User's obligations

- 3.1 The User will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with hackajob's written instructions. The User will not process the Personal Data for any other purpose or in a way that does not comply with this Annex or the Data Protection Legislation. The User will promptly notify the hackajob if, in its opinion, hackajob's instructions do not comply with the Data Protection Legislation.
- 3.2 The User must comply promptly with any of your written instructions requiring it to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 3.3 The User will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless you specifically authorise the disclosure, or as required by domestic law, court or regulator (including the Commissioner). If a domestic law, court or regulator (including the Commissioner) requires us to process or disclose the Personal Data to a third-party, The User must first inform you of such legal or regulatory requirement and give you an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.
- 3.4 The User will reasonably assist hackajob, at no additional cost, with meeting its compliance obligations under the Data Protection Legislation, taking into account the nature of the User's processing and the information available to us, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner under the Data Protection Legislation.
- 3.5 hackajob must notify the User promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the User's performance of this Annex.

4. User's employees

4.1 We will ensure that all of our employees:

- (a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;
- (b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and
- (c) are aware both of the User's duties and their personal duties and obligations under the Data Protection Legislation and this Annex.

5. Security

5.1 The User must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful

loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Part B.

- 5.2 The User must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:
- (a) the pseudonymisation and encryption of personal data;
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

- 6.1 The User will within 24 hours and in any event without undue delay notify you in writing if it becomes aware of:
- (a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data.
 - (b) any accidental, unauthorised or unlawful processing of the Personal Data; or
 - (c) any Personal Data Breach.
- 6.2 Where the User becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide hackajob with the following written information:
- (a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;
 - (b) the likely consequences; and
 - (c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.
- 6.3 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, we will co-ordinate with each other to investigate the matter. Further, hackajob will reasonably co-operate with you at no additional cost, in the User's handling of the matter, including but not limited to:
- (a) assisting with any investigation;
 - (b) providing hackajob with physical access to any facilities and operations affected;
 - (c) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by hackajob; and
 - (d) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.
- 6.4 The User will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the hackajob's written consent, except when required to do so by domestic law.
- 6.5 The User agrees that hackajob has the sole right to determine:
- (a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope

regulators, law enforcement agencies or others, as required by law or regulation or in the User's discretion, including the contents and delivery method of the notice; and

- (b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 The User will cover all reasonable expenses associated with the performance of the obligations under 6.1 to 6.3 unless the matter arose from the hackajob's specific written instructions, negligence, wilful default or breach of the Terms of Use, in which case hackajob will cover all reasonable expenses.

7. Cross-border transfers of personal data

7.1 The User (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK and EEA without obtaining the hackajob's prior written consent. Personal Data may be stored in the EU in compliance with the User's agreement(s) with sub-contractors.

8. Subcontractors

8.1 The User uses the sub-contractors listed at Part A to process Personal Data. The User will give hackajob notice of any additional sub-contractors and hackajob will have an opportunity to object to the appointment of a sub-contractor.

8.2 The User maintains control over all of the Personal Data it entrusts to a subcontractor and takes responsibility for a sub-contractor's acts and omissions.

9. Complaints, data subject requests and third-party rights

9.1 The User must, at no additional cost to hackajob, take such technical and organisational measures as may be appropriate, and promptly provide such information to you as you may reasonably require, to enable hackajob to comply with:

- (a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and
- (b) information or assessment notices served on you by the Commissioner under the Data Protection Legislation.

9.2 The User must notify hackajob immediately in writing if we receive any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The User must notify hackajob within five days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The User will give hackajob, at no additional cost, our full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The User must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the User's written instructions, or as required by domestic law.

10. Term

10.1 This Annex will remain in full force and effect so long as we retain any of the Personal Data related to the Terms of Use in our possession or control (**Term**).

- 10.2 The User's failure to comply with the terms of this Annex is a material breach of the Terms.
- 10.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation, either party may terminate the relationship on written notice to the other party.

11. Data return and destruction

- 11.1 The User will give hackajob, or a third-party nominated in writing by hackajob, a copy of or access to all or part of the Personal Data in your possession or control in the format and on the media reasonably specified by Hackajob.
- 11.2 On termination of the relationship, the User will securely delete or destroy or, if directed in writing by hackajob, return and not retain, all or any of the Personal Data related to this Annex in its possession or control, except for one copy that we may retain and use for internal compliance reasons only if it is necessary to do so. Any retained Personal Data will remain subject to confidentiality provisions in the Terms.
- 11.3 If any law, regulation, or government or regulatory body requires the User to retain any documents, materials or Personal Data that the User would otherwise be required to return or destroy, it will notify hackajob in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

12. Records

- 12.1 The User will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in 5.1 (**Records**).
- 12.2 The User will ensure that the Records are sufficient to enable hackajob to verify its compliance with our obligations under this Annex and the Data Protection Legislation and The User will provide hackajob with copies of the Records upon request.

13. Audit

- 13.1 The User will permit hackajob and its third-party representatives to audit The User's compliance with its obligations under this Annex, on at least 10 days' notice, during the Term. Subject to confidentiality restrictions, The User will give Hackajob and its third-party representatives all necessary assistance to conduct such audits at no additional cost to you. The assistance may include, but is not limited to:
- (a) physical access to, remote electronic access to, and copies of the Records and any other information held at The User's premises or on systems storing the Personal Data;
 - (b) access to and meetings with any of our personnel reasonably necessary to provide all explanations and perform the audit effectively; and
 - (c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to process the Personal Data.
- 13.2 The notice requirements in 13.1 will not apply if hackajob reasonably believes that a Personal Data Breach has occurred or is occurring, or that we are in material breach of any of its obligations under this Annex or any of the Data Protection Legislation.

14. Warranties

14.1 The User warrants that:

- (a) its employees, subcontractors, agents and any other person or persons accessing the Personal Data on our behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;
- (b) we and anyone operating on our behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;
- (c) we have no reason to believe that the Data Protection Legislation prevents us from providing any of the services in the Terms; and
- (d) considering the current technology environment and implementation costs, we will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:
 - (i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;
 - (ii) the nature of the Personal Data protected; and
 - (iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in 5.1.

14.2 hackajob warrants and represent that The User's expected use of the Personal Data for the Business Purposes and as specifically instructed by hackajob will comply with the Data Protection Legislation.

15. Notice

15.1 Any notice given to The User under or in connection with this Annex must be in writing (including e mail) and delivered to:

Scott Simpson
Data Protection Officer
DPO@hackajob.co

PART A: Personal Data processing purposes and details

Subject matter of processing: We are processing the personal data to help candidates find employment with our clients through our online SaaS platform

Duration of Processing: *As long as a User uses the Services.*

Nature of Processing: *Collection, storage and transmission of Personal Data between Candidates and Employers.*

Business Purposes: *Provision of on-line career services and connection between candidates and employees.*

Personal Data Categories:

- For Candidates we capture the following data fields:
 - Full Name
 - Phone Number
 - Email Address
 - University
 - Skills
 - Location
 - Salary
 - Visa status
 - Work experience

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

Data Subject Types: *Candidates and employers.*

Approved Subcontractors/Subprocessors:

- Heap Analytics - creating reports
- Close.io - CRM - calling candidates
- Active Campaign - Marketing campaigns - sending newsletters to candidates and clients
- Salesforce - CRM - tracking the opportunities
- DataDog - monitoring - tracking errors from the application

PART B: Security measures

Insert description of its technical and organisational data security measures such as:

- Physical access controls - access control system for the office, alarms and CCTV
- System access controls - all the data are encrypted and all the systems have passwords and 2FA
- Data access controls - Everyone have access only to the data they need to have based on permission
- Transmission controls - Every request is encrypted with TLSv1.2_2021
- Input controls - we are validating the data and storing in the database only if the input is valid
- Data backups - Daily or hourly depends on how critical is the system for which is the backup, backups are encrypted and kept for 15 days
- Data segregation - Every client has his own identifier in our systems and we are validating and returning only the data associated with the identifier