Tracer Management Systems Limited trading as Joblogic

Data Processing Addendum

1. Introduction

1.1 This Data Processing Addendum forms part of each Master Services Agreement entered into between Joblogic and the Customer and is subject to its terms and conditions, including the limitations and exclusions of liability, set out therein. In the event of any conflict between this Data Processing Addendum and the Master Services Agreement, this Data Processing Addendum shall prevail in respect of data protection matters.

1.2 Definitions for capitalised terms used in this Addendum are set out in clause 5.

2. Compliance with Data Protection Law

Each party shall comply with its respective obligations under applicable Data Protection Laws. This Addendum is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Law.

3. Data processing

3.1 The Customer and Joblogic acknowledge that Joblogic will perform certain processing activities, the subject matter, duration, nature and purpose of which are described more fully in the Appendix 1 to this Data Processing Addendum (the "**Description of Processing**"). In respect of such processing activities, Joblogic is the processor and the Customer is the controller.

3.1.1 For the purposes of this Data Processing Addendum:

3.1.2 Joblogic acts as a processor on behalf of the Customer in respect of all Customer Personal Data processed in connection with the provision of the Services.

3.1.3 Joblogic acts as an independent controller in respect of Aggregated and Analytical Data and Business Data processed for analytics, benchmarking and service improvement purposes. Such data does not constitute Customer Personal Data and does not constitute personal data.

3.2 The Customer retains control of the personal data and shall be responsible for establishing and maintaining the lawful basis for the processing of personal data under the Master Services Agreement and providing appropriate privacy notices to its employees and other personnel in respect of the Services and obtaining any required consents, and for the written processing instructions it provides to Joblogic.

3.3 The Customer shall not provide or disclose any special categories of personal data to Joblogic for processing unless such processing is necessary for the use of the Services and documented in Appendix 1, and the Customer shall ensure that any such processing complies with applicable Data Protection Law.

3.4 In respect of this Data Processing Addendum, Joblogic shall:

(a) only process the personal data in accordance with the Description of Processing or other written instructions from the Customer, unless such processing is required by any law to which Joblogic is subject, in which case, Joblogic shall (to the extent permitted by law) inform the Customer of that legal requirement before carrying out the processing;

(b) process the personal data only to the extent, and in such a manner, as is necessary for the purposes of carrying out its obligations under the Master Services Agreement;

(c) ensure that persons engaged in the processing of personal data are bound by appropriate confidentiality obligations;

(d) implement and have in place appropriate technical and organisational measures to protect against unauthorised, unlawful or accidental processing, including accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, such measures in each case to be appropriate to the likelihood and severity of harm to data subjects that might result from the unauthorised, unlawful or accidental processing, having regard to the state of technological development and the cost of implementing any measures, a summary of which is set out in the Security Measures and the Customer acknowledges that the Security Measures are subject to technical progress and development and that Joblogic may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services;

(e) engage sub-processors to process Customer Personal Data, provided that the Customer grants Joblogic a general authorisation to do so. Joblogic shall ensure that any sub-processor is subject to written obligations that are materially equivalent to those set out in this Data Processing Addendum.

(f) comply promptly with any lawful request from the Customer requesting access to, copies of, or the amendment, transfer or deletion of the personal data to the extent the same is necessary to allow the Customer to fulfil its own obligations under the Data Protection Law, including the Customer's obligations arising in respect of a request from a data subject;

(g) notify the Customer promptly if it receives any complaint, notice or communication (whether from a data subject, competent supervisory authority or otherwise) relating to the processing, the personal data or to either party's compliance with the Data Protection Law as it relates to this Master Services Agreement, and provide the Customer with reasonable co-operation, information and other assistance in relation to any such complaint, notice or communication;

(h) notify the Customer without undue delay if Joblogic becomes aware that an instruction from the Customer, as applied to the processing of Customer Personal Data under this Data Processing Addendum, is manifestly unlawful under applicable Data Protection Law or cannot be complied with due to a legal requirement binding on Joblogic. For the avoidance of doubt, Joblogic is not responsible for assessing or monitoring the legal sufficiency of the Customer's processing activities or instructions and does not provide legal advice;

(i) inform the Customer without undue delay after becoming aware that any personal data processed under this Master Services Agreement has been lost or destroyed or has

become damaged, corrupted, or unusable or has otherwise been subject to unauthorised or unlawful processing including unauthorised or unlawful access or disclosure;

(j) inform the Customer promptly if it receives a request from a data subject for access to that person's personal data and shall not disclose the personal data to any data subject (or to any third party) other than at the request of the Customer or as otherwise required under this Master Services Agreement;

(k) where the Customer is unable to use the self-service functionality within the Services to access a data subject's personal data, promptly provide the Customer with reasonable co-operation and assistance in relation to a data subject request;

(l) provide reasonable assistance to the Customer in responding to requests from data subjects and in assisting the Customer to comply with its obligations under Data Protection Law with respect to security, breach notifications, data protection impact assessments and consultations with supervisory authorities or regulators;

(m) delete or return that personal data to the Customer at the end of the duration of the processing as referred to in the Appendix 1, and at that time delete or destroy existing copies (unless otherwise required by law or to the extent the personal data is part of Joblogic's regular back-up or archive systems, subject to continued compliance with this Data Processing Addendum);

(n) subject to the requirements of commercial and client confidentiality, make available to the Customer on request a copy of any third-party audit report demonstrating Joblogic's compliance with Data Protection Laws, and such further information reasonably required to demonstrate compliance with this Data Processing Addendum. If the Customer requires further information which is not included as part of the third party audit report or further information, Joblogic shall allow for and contribute to audits, including inspections, of compliance with this Data Processing Addendum conducted by the Customer or a professional independent auditor engaged by the Customer subject to the conditions of this Data Processing Addendum. The following requirements apply to any audit: (i) the Customer must give a minimum of 30 days' notice of its intention to audit (or such shorter period of notice as it receives itself where an audit is mandated by its regulator); (ii) the Customer may exercise the right to audit no more than once in any calendar year; (iii) commencement of the audit shall be subject to agreement with Joblogic of a scope of work for the audit at least 10 days in advance; (iv) Joblogic may restrict access to certain parts of its or its sub-processors facilities and certain records where such restriction is necessary for commercial and/or client confidentiality; (v) the audit shall not include penetration testing, vulnerability scanning, or other security tests; (vi) the right to audit includes the right to inspect but not copy or otherwise remove any records, other than those that relate specifically and exclusively to the Customer; (vii) any independent auditor will be required to sign such non-disclosure agreement as is reasonably required by Joblogic prior to the audit; (viii) the audit shall be conducted during normal business hours and shall not cause disruption to Joblogic's business; and (ix) the Customer shall compensate Joblogic for its reasonable costs (including for the time of its personnel, other than the 'Main contact' specified in the Order Form) incurred in supporting any audit. All reports, findings, and information provided or resulting from any such audit shall be considered Joblogic's Confidential Information;

(o) provide assistance to the Customer with any data privacy impact assessments for which the Customer shall compensate Joblogic for its reasonable costs (including for the time of its personnel, other than the 'Main contact' specified in the Order Form) incurred in supporting any data privacy impact assessments; and

(p) only transfer personal data outside UK and/or the EEA if such transfer is carried out in accordance with clause 4.

4. International transfers

4.1 The parties agree that when the transfer of personal data from the Customer to Joblogic is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) in relation to personal data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes shall be as set out in Clause 3.4(e) of this Addendum;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Appendix I to this Addendum;

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in clause 3.4(d) to this Addendum.

(b) in relation to personal data that is protected by the UK GDPR, the UK Addendum will apply completed as follows:

(i) the EU SCCs, completed as set out above in clause 4.1(a) of this Addendum shall also apply to transfers of such Data, subject to sub-clause (ii) below;

(ii) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this Addendum.

(c) in the event that any provision of this Addendum contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

4.2 Joblogic shall not participate in (nor permit any sub-processor to participate in) any other Restricted Transfers of personal data (whether as an exporter or an importer of the Data) unless the Restricted

Transfer is made in full compliance with applicable Data Protection Law and pursuant to Standard Contractual Clauses implemented between the relevant exporter and importer of the personal data.

5. California Personal Data Requirements

5.1 With respect to personal data relating to a data subject residing in California and that is subject to the CCPA ("California Personal Data"), Joblogic agrees to:

5.1.1 not (i) process California Personal Data outside of the direct relationship between Joblogic and Customer unless otherwise permitted by Data Protection Laws, (ii) sell or share California Personal Data shall; or (iii) combine California Personal Data Processed pursuant to the Agreement with personal data received from other sources without the prior consent of Customer or as otherwise permitted by Data Protection Laws.

5.1.2 where Joblogic independently determines that it can no longer comply with Data Protection Laws, promptly provide notice to Customer;

5.1.3 through the processes set forth in Section 3.4(n), provide Customer with reasonable and appropriate means through which Customer can ensure California Personal Data is used in a manner consistent with Data Protection Laws.

6. Definitions

In this Addendum, the following terms have the meanings given to them below, unless a contrary intention appears:

Master Services Agreement or MSA means the master services agreement entered into between Joblogic and the Customer governing the provision of the Services, together with any order forms or schedules incorporated into it.

Services has the meaning given to it in the Master Services Agreement.

Appendix means an appendix to this Data Processing Addendum.

The terms personal data, business, service provider, controller, processor, process and data subject have the meanings given to them under Data Protection Law (including, for example, materially equivalent terms (for example, "personal data" includes terms defined as "personal information" under Data Protection Law)).

Customer Personal Data means personal data processed by Joblogic on behalf of the Customer in its capacity as processor under this Data Processing Addendum.

Business Data means data relating to a customer's business operations, services, jobs, assets, workflows, usage patterns or performance metrics that does not relate to an identified or identifiable natural person.

Aggregated and Analytical Data means data derived from Business Data and/or Service usage that is aggregated or de-identified and combined across customers or services for analytics, benchmarking, reporting and service improvement, and which does not constitute personal data under applicable Data Protection Law.

Business Day means a day not being a Saturday, Sunday, bank or public holiday on which trading banks are generally open for business in London.

Data Protection Law means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

Restricted Transfer means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018;

Security Measures means the security measures detailed within Appendix 1;

Standard Contractual Clauses means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 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 ("**EU SCCs**"); and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**").

Appendix 1 - Description of Processing

This Appendix 1 forms part of the Addendum and describes the processing that the processor will perform on behalf of the controller.

A. LIST OF PARTIES

Controller(s) / Data exporter(s): [*Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1.	Name:	Customer as identified in the Order Form and/or Master Services Agreement.
	Address:	See Order Form/Master Services Agreement
	Contact person's name, position and contact details:	As specified in Order Form/Master Services Agreement
	Activities relevant to the data transferred under these Clauses:	Provision of Services
	Signature and date:	See Order Form/Master Services Agreement
	Role (controller/processor):	Controller

Processor(s) / Data importer(s): *[Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection*]

1.	Name:	Tracer Management Systems Limited trading as Joblogic 03611671
	Address:	305 Zellig Custard Factory, Gibb Street Digbeth, Birmingham, B9 4AA, United Kingdom
	Activities relevant to the data transferred under these Clauses:	Provision of Services
	Signature and date:	See Order Form/Master Services Agreement
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Customer's employees
Categories of personal data transferred:	This will depend on the particular service provided to the Customer but may include the following categories of data: End users/customers of Joblogic Group Customers • Personal details: name, surname and contact details (e.g., business address, delivery address, phone number, email address fax number(s)). • Financial information: bank account details. • Order data: purchasing, return and cancellation history; buyer preferences. • User behaviour for the purpose of advertising and providing personalised programs, apps, content and other products and services. • IT information: user log and information from the products and services. • Employees of Joblogic Group Customers • Personal details: name; date and place of birth; gender; marital status; dependents;

	religion; education and qualification details; security information (access levels and passwords); medical information; work related travel information; dietary requirements; information about criminal convictions and offences; background check results. • Identification data: civil/marital status, photograph, nationality, corporate identifier. • Contact details: address, telephone number, email address, fax number, emergency contact information. • Employment details: job title, company name, grade, occupation code, geographic location, employee performance and evaluation data; employee discipline information; information regarding previous roles and employment, employee benefits information such as election decisions, leave requests, authorisation/declination, health insurance company. • IT-related data: computer ID, user ID and password, domain name, IP address, log files, software and hardware inventory, software usage pattern tracking information.
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:	Joblogic does not require or permit entry of special category data unless explicitly agreed in writing.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous
Nature of the processing:	Such processing as is necessary to enable Joblogic to provide the ordered Services to the Customer
Purpose(s) of the data transfer and further processing:	The performance of Joblogic's obligations and the exercise of its rights in respect of the ordered Services
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	The duration of the Master Services Agreement or longer as: (i) is specified in any provisions of this Master Services Agreement regarding data retention; and (ii) is required for compliance with law
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	As Required

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	Information Commissioners Office, United Kingdom

D. SUB-PROCESSORS

The Customer authorises Joblogic to engage sub-processors to process Customer Personal Data in connection with the provision of the Services. Joblogic shall ensure that any such sub-processor is subject to written obligations that provide a level of data protection that is no less protective than those set out in the Data Processing Addendum. Joblogic may add, replace or remove sub-processors from time to time, subject to the notification and objection mechanism set out in the Data Processing Addendum.

E. SECURITY MEASURES – Joblogic Product

1. Encryption
    a. Data in transit is encrypted
    b. Data at rest is encrypted

2. Access Authorisation, Passwords and Authentication
    a. Access authorisations and password complexity rules
    b. MFA / 2FA is supported

3. Back ups
    a. Performed regularly for all production systems
    b. Tested regularly
    c. Hosted offsite at different geographical locations

4. Testing
    a. Third Party penetration tests performed regularly
    b. Automated software security Scans performed weekly