MORGAN MCKINLEY

TERMS AND CONDITIONS FOR RECRUITMENT SOLUTIONS

February 01, 2023

ATTACHMENT A

DATA PROCESSING AGREEMENT

APPLICABLE IF BACKGROUND SCREENING ADD-ON SERVICES FOR TEMPORARY WORKERS OR CONTRACTORS IS AGREED BETWEEN THE PARTIES PURSUANT TO RECRUITMENT SOLUTIONS T&C

1. TABLE OF CONTENTS

2. INTRODUCTION

This Data Protection Agreement, including its Schedules (the "**DPA**") forms part of the Terms of and Conditions for Recruitment Solutions (the "T&C") attached or incorporated by reference, including the SCCs, as defined and linked below, and is applicable only in relation to Background Screening Add-On Services for Temporary Workers or Contractors as set out in Schedule A and agreed between the Parties under the T&C ("Add-On Services") in relation to clause 10.3 of the General Terms. The Parties acknowledge that outside of the Personal Data set forth in Schedule A ROPA, the Parties are generally acting as independent Controllers and as such, are outside the scope of this DPA.

By accepting Morgan McKinley T&C, this DPA is entered into by the Morgan McKinley Client identified in the new client set up document for Add-On Services and Premier Recruitment International UC trading as Morgan McKinley and governs the processing of Personal Data by Morgan McKinley on behalf of the Client in connection with the Add-On Services as defined above. In the event of any conflict or inconsistency between (i) the SCC, (ii) this DPA, and (iii) the T&C, the document appearing first in the list shall take precedence.

3. DEFINITIONS

3.1. The following definitions apply for the purposes of this Addendum:

    3.1.1. "**Data Protection Law**" means any data protection laws applicable to the processing of personal data contemplated by the T&C including, without limitation, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**") and any other applicable legislation, decision, statutory instrument or regulation in force at present or which comes into force;

    3.1.2. "**EEA**" or "**European Economic Area**" means the European Economic Area that combines the countries of the European Union together with Iceland, Norway and Liechtenstein;

    3.1.3. "**Morgan McKinley**" means Premier Recruitment International UC t/a Morgan McKinley, of 6th Floor Penrose Dock 2, Alfred Street, Victorian Quarter, Cork T23YY09, company registration number 131679 including our associated bodies corporate.

    3.1.4. "**Personal Data**" means any information processed by Morgan McKinley as part of Add-On Services as defined above, relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

    3.1.5. "**Sub-Processor**" means, in any case where Morgan McKinley acts as a Processor hereunder, any third-party subcontractor or affiliate of Morgan McKinley engaged by Morgan McKinley to Process Personal Data.

    3.1.6. "**Standard Contractual Clauses**" means the standard contractual clauses as approved by the European Commission in Decision (EU) 20211/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, as amended or replaced from time to time and set out in the Official Journal of the European Union's relevant website and available for reference here: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0915&rid=7. To the extent the Parties enter into the SCC under the T&C, the SCC is set out here.

    3.1.7. "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to Article 51 of the GDPR.

3.2 "**Data Subject**", "**Controller**", "**Processor**" and "**Processing**" shall have the meanings given to them in the relevant Data Protection Law and their cognate terms shall be construed accordingly.

3.3. Capitalised terms used herein, but not defined shall have the meaning provided in the T&C.

3.4. Unless required under Data Protection Law, nothing in this DPA reduces either party's obligations under the T&C in relation to the protection of Personal Data.

4. PROCESSING OF PERSONAL DATA

4.1 Details of Processing and Roles of the Parties. The parties acknowledge and agree that with regards to the subject matter of Processing of Personal Data, the types of Personal Data and categories of Data Subjects within the scope of this DPA is described in Schedule A ROPA to this DPA. To this extent, the Client is the Controller, Morgan McKinley is the Processor, and that Morgan McKinley affiliates, or third parties engaged by Morgan McKinley pursuant to the requirements set forth in clause 8 are Sub-Processors.

4.2 Morgan McKinley's Processing of Personal Data. Morgan McKinley shall Process Personal Data on behalf of and in accordance with Client's documented instructions as follows: (i) Processing in accordance with the T&C and/or assignment schedule(s); (ii) Processing initiated by the Client in their use of the Add-On Services; and (iii) Processing to comply with other documented reasonable instructions provided by Client (whether via email or at the time of booking a Temporary Worker or Contractor) where such instructions are consistent with the terms of the T&C, unless otherwise prohibited or in the opinion of Morgan McKinley is unlawful under Data Protection Law to which Morgan McKinley is subject. Morgan McKinley shall inform the Client if, in Morgan McKinley's opinion, such instruction infringes any Data Protection Law.

4.3 No Commercial Use of Personal Data. Morgan McKinley shall not sell or use Personal Data for any purpose other than to perform the Add-On Services.

4.4 Client Obligations Regarding Personal Data. Client agrees to (i) determine the purpose and lawful basis of Morgan McKinley's Processing of Personal Data on Client's behalf; (ii)ensure its instructions for the Processing of Personal Data comply with Data Protection Law; and (iii) shall comply itself with all relevant Data Protection Law, including any applicable requirements to provide notice to and/or obtain consent from Data Subjects for Processing by Morgan McKinley.

5.   **MORGAN MCKINLEY PERSONNEL**

5.1 Access Controls. Morgan McKinley shall ensure that access is limited to those officers, employees, agents, and subcontractors on a "need to know" basis where access is necessary to perform obligations under the T&C or exercise its rights herein under this DPA.

5.2 Confidentiality. Morgan McKinley shall ensure all staff Processing Personal Data are subject to a duty of confidentiality and that they process Personal Data only for the purposes of delivering the Add-On Services within the scope of this DPA.

5.3 Personnel. Morgan McKinley shall take reasonable steps to ensure the reliability of staff engaged in the Processing Personal Data.

6.   **SECURITY**

6.1 Controls. Morgan McKinley shall use appropriate technical and organisational measures designed to protect Personal Data against any misuse, accidental, unlawful, or unauthorised destruction, loss, alteration, disclosure, acquisition, or access, including the use of Sub-Processors with industry recognised security standards such as ISO 27001 or similar recognised standards.

6.2 Sub-Processor Certifications. Morgan McKinley has, where possible, obtained the relevant third-party certifications of its Sub-Processors and upon Client's written request, and subject to the confidentiality obligations set forth in its agreement with its Sub-Processor, shall make available to Client a copy of the most recent third-party certifications.

6.3 Data Protection Impact Assessment. Where appropriate, Morgan McKinley will reasonably cooperate and assist with a Client's request to carry out a data protection impact assessment related to Client's use of the Service.

6.4 Security Incident Management. Morgan McKinley will notify the Client of any Personal Data breach by Morgan McKinley or its Sub-Processors without due delay and in any event within 48 hours of becoming aware of a Personal Data breach. Morgan McKinley shall make reasonable efforts to identify the cause of the Personal Data breach and remediate the cause of the breach to the extent it is within its control, excluding any Personal Data breach caused by the Client.

7.   **ASSISTANCE TO CONTROLLER**

7.1 **Data Subject Requests.** Morgan McKinley shall notify the Client within ten (10) calendar days if it receives a Data Subject access request, including requests by the Data Subject to exercise rights in respect of access, rectification, erasure, restriction, portability blocking or deletion, and shall provide the Client with full details. Morgan McKinley shall cooperate as requested by the Client to enable the Client to comply with any exercise of rights by a Data Subject regarding Personal Data within the scope of this DPA.

7.2. **Request from Third Parties**. Morgan McKinley shall, where permitted by law, promptly notify the Client if it receives any information request, notice or investigation from a third party, including a Supervisory Authority or other government agency. Morgan McKinley shall only respond to the requesting party if required by law to do so and will make reasonable efforts to work with the requesting party to narrow the scope of the Personal Data included in the request.

8.   **SUB-PROCESSORS**

8.1 Current Sub-Processors. Morgan McKinley's current list of Sub-Processors for the Add-On Services, which includes affiliates, and third parties is identified in Schedule B of this DPA. Morgan McKinley shall notify the Client in writing of any new Sub-Processor.

8.2 Appointment of New Sub-Processor. Client acknowledges and grants Morgan McKinley a general authorisation to appoint third-party Sub-Processors in connection with the Add-On Services, on the understanding that Morgan McKinley has entered into a written agreement with each Sub-Processor containing data protection obligations not less protective than those in this DPA to the extent applicable to the services provided by such Sub-Processor.

8.3 Objection Right. Client may reasonably object to Morgan McKinley's use of a new Sub-Processor by notifying Morgan McKinley in writing within 30 days after receipt of a notice of a new appointment. Morgan McKinley will use commercially reasonable efforts to make available to Client a change in Add-On Services that is satisfactory to the Client. If Morgan McKinley is unable to facilitate such change, the Client may terminate the T&C with 30 days written notice.

9.   **DATA TRANSFERS**

The Client acknowledges and agrees that Personal Data Processed as part of the Add-On Services may be transferred by Morgan McKinley to, used, and stored outside of the EU, Switzerland, the UK, as set forth in Schedule B Sub-Processor list, to the extent Morgan McKinley ensures such transfer is in accordance with Data Protection Law and with any applicable transfer mechanism provisions approved and adopted by the GDPR including:

   (i)   To the extent Morgan McKinley has adopted approved Binding Corporate Rules for intragroup transfers, if applicable;

   (ii)   In accordance with approved SCC, where relevant; and/or

   (iii)   The recipient of the Personal Data is in a country or territory that has been found to ensure an adequate level of protection for the Data Subject.

10. **AUDIT**

Morgan McKinley shall, at Client's written request, and subject to the confidentiality obligations in the T&C, make available to the Client information regarding Morgan McKinley's compliance with this DPA in the form of standardised security questionnaires, third-party certifications and audit reports where possible.

11. **RETURN AND DELETION OF PERSONAL DATA**

   Morgan McKinley shall return and/or delete Personal Data upon written request from the Client to the extent allowed by applicable law, in accordance with the procedures and timeframes agreed by the Parties.

12. **LIMITATION OF LIABILITY**

   The aggregate liability of either Party for liability arising out of or relating to this DPA, shall be governed by the Limitation of Liability section of the T&C and shall apply in the aggregate for all claims under both the T&C and this DPA.

13. **TERM**

   This DPA shall remain in effect as long as Morgan McKinley carried out Personal Data Processing activities on behalf of the Client or until the termination of the T&C and all Personal Data has been returned or deleted in accordance with this DPA.

14. **GOVERNING LAW AND JURISDICTION**

   This DPA shall be governed by the laws of Ireland, and any action or proceeding related to this DPA will be brought in Ireland.

SCHEDULE A – RECORD OF PROCESSING ACTIVITIES (ROPA)

ROPA	
Subject Matter	Applicable for Add-On Background and Screening Services for Temporary Workers and/or Contractors only
Duration and Frequency of Processing	Morgan McKinley will Process Personal Data for the duration of the T&C, unless agreed otherwise in writing. Frequency of Processing is dependent on Client requests for such Add-On Services
Nature and purpose of Processing	The Client determines the components and dept of the Add-On Background and Screening Services that it engages Morgan McKinley to provide as an Add-On Service on its behalf prior to an Engagement of a Temporary Worker and/or Contractor in accordance with the T&C, this DPA, and Data Protection Law.
Types of Personal Data	As each Background and Screening requirement is subject to vary depending on the requirements of the Client and assignment requirements against which the Temporary Worker and/or Contractor is Engaged for, below is a general list of Checks that may apply for this DPA: ● **Identity check** ● **Right to Work Check** ● **Peps and Sanctions Check** ● **Reference Check** ● **Education Check** ● **Other Checks as agreed between the Parties and as allowed by law** *Please note that criminal background checks/declarations and/or medical checks or examinations cannot generally be facilitated by Morgan McKinley.*
Categories of Data Subjects	Temporary Workers Contractors

SCHEDULE B – Sub-Processor List

Affiliate Sub-Processor List for Add-On Background Screening and Compliance Checks			
Full Entity Name	**Location of Processing**	**Purpose of Processing**	**Transfer Mechanism**
Morgan McKinley Group Ltd	UK	In some instances, our UK compliance team may assist our Irish compliance team with completing certain Add-On Background Screening and Compliance Checks	Adequacy Country
Morgan McKinley Services Pvt	India	Provides business support services as part of our global structure	SCC

Third Party Sub-Processor List for Add-On Background Screening and Compliance Checks			
Google LLC	All locations in this link are possible: https://www.google.com/about/datacenters/locations/	Email and workspace SaaS provider.	SCC
Access UK Limited	EU/UK	Primary background screening and compliance vendor	Adequacy Country
HireRight Limited	UK	Background screening and compliance vendor	Adequacy

ATTACHMENT A To Morgan McKinley Recruitment Solutions T&C

		used in limited circumstances on request of the Client	Country
Freshdesk Inc	USA	Ticking and support system used in certain instances to communicate or collect additional Background Screening and Compliance Checks from Temporary Workers and/or Contractors	SCC

SCHEDULE C: TECHNICAL AND ORGANISATIONAL MEASURES

The Parties agree to each implement at a minimum standard the following measures to ensure the security of the data:

1. **Organisational management** and dedicated staff will be responsible for the development, implementation, and maintenance of its respective information security programs.
2. **Audit and risk assessment** procedures for the purposes of periodic review and assessment of risks to the party's organization, monitoring and maintaining compliance with its policies and procedures, and reporting the condition of its information security and compliance to senior internal management.
3. **Regular review**: Maintain Information security policies and make sure that policies and measures are regularly reviewed and where necessary, improve them.
4. **Communication** with applications utilising cryptographic protocols such as TLS to protect information in transit over public networks. At the network edge, stateful firewalls, web application firewalls, and DDoS protection are used to filter attacks. Within the internal network, applications follow a multi-tiered model which provides the ability to apply security controls between each layer.
5. **Data security controls** which include logical segregation of data, restricted (e.g., role-based) access and monitoring, and where applicable, utilisation of commercially available and industry-standard encryption technologies.
6. **Logical access controls** designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).
7. **Password controls** designed to manage and control password strength, and usage including prohibiting users from sharing passwords.Multi Factor Authentication is required for all remote and on-premises access to company systems and data, including email, cloud-based applications, and VPN.
8. **Event Logging:** System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.
9. **Physical and environmental security** of data centres, server room facilities and other areas containing confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log movement of persons into and out of Data centre facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
10. **Operational Control Management:** Operational procedures and controls to provide for configuration, monitoring, and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from its possession.
11. **Change management** procedures and tracking mechanisms designed to test, approve, and monitor all changes to technology and information assets.
12. **Incident / problem management** procedures designed to allow investigation, respond to, mitigate, and notify of events related to Morgan McKinley technology and information assets.
13. **Network security controls** that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
14. **Patch management**: vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses and other malicious code.
15. **Business resiliency/continuity and disaster recovery procedures**, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters.
16. **Management of Cloud** Vendors to ensure that they are following their own Technical and Organisational Measures and protect Morgan McKinley's sensitive data to the highest Industry standards.