Last Updated: 1 April 2025

This Data Protection Addendum ("**DPA**") forms part of the agreement ("**Agreement**") between the Security Watchdog Limited, trading as Security Watchdog ("**SW**") under which SW provides Customer (as defined in the Agreement and hereinafter "**Customer**") certain products or services ("**Service**s") and in which this DPA is referenced. Each a "**Party**" and together the "**Parties**")

THE PARTIES AGREE as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 The definitions and rules of interpretation in this Clause apply in this Agreement.

"**Candidate**" means a person put forward by the Customer as being already employed by, previously employed by or who has been offered employment or contractual engagement by the Customer or any other person in respect of whom the Customer requests SW to provide Services.

"**Customer Data**" means data, information and documentation in whatever form or medium belonging to the Customer, as provided by the Customer and used by SW in the provision of the Services.

"**Data Protection Laws**" means the following legislation to the extent applicable from time to time: (a) the UK GDPR, Data Protection Act 2018 and Privacy and Electronic Communications (EC Directive) Regulations 2003; (b) the EU GDPR and any national law issued under that regulation; and (c) any laws or regulations that replace or supersede the legislation referred to in (a) to (b) from time to time. The terms "**Data Controller**", "**Data Processor**", "**Data Subject**" and "**Personal Data**" are as defined in the Data Protection Laws.

"**International Transfer Clauses**" means (i) standard data protection clauses issued by the United Kingdom Information Commissioner under Section 119A(1) Data Protection Act 2018, insofar as they apply to Restricted Transfers including (but not limited to) the International Data Transfer Agreement (VERSION A1.0, in force 21 March 2022); or (ii) module 3 (processor to processor) of the standard contractual clauses for the transfer of personal data to third countries pursuant to the EU Commission Implementing Decision (2021/914/EU) of 4 June 2021 under Regulation (EU) 2016/679 together with the United Kingdom Information Commissioner's approved International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (VERSION B1.0, in force 21 March 2022).

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Personal Data transmitted, stored or otherwise processed.

"**Processing**" has the meaning set out in the Data Protection Laws and for the purposes of this DPA, "**process**" and "**processed**" will be interpreted accordingly.

"**Supervisory Authority**" means any regulatory authority responsible for the enforcement, regulation or governance of any Data Protection Laws and any replacement or successor body or person for any such authority from time to time.

"**Sub-Processors**" means third party processors explicitly identified on the Sub-Processor page and/or any other sub-processor as SW may notify Customer from time to time in writing.

2 SCOPE

2.1 This DPA sets out the data privacy obligations of both Parties under the Agreement. in relation to the Services provided under this Agreement. Each Party warrants to the other that it will comply with all applicable Data Protection Laws in respect of its Processing of Personal Data.

3 ROLES AND RESPONSIBILITIES

3.1 SW is a Data Processor and the Customer is a Data Controller and their respective obligations under this DPA shall be in accordance with those roles.

3.2 Appendix 1 to this DPA sets out the data processing particulars relating to the Agreement, including categories of Personal Data and Data Subjects.

3.3 SW shall only process Personal Data on the documented instructions of Customer (as set out in or varied from time to time in accordance with the Agreement, and which shall include the provision of Services) unless required to process that Personal Data for other purposes by relevant law. Where such a requirement is placed on SW, it shall provide prior notice to Customer unless the relevant law prohibits the giving of notice on important grounds of public interest.

3.4 SW will inform Customer if, in its opinion, Customer's instructions would be in breach of Data Protection Laws.

3.5 The Customer shall ensure that, when using the Services or accessing the System, any Personal Data have been collected, uploaded and disclosed in accordance with the Data Protection Laws. The Customer shall further ensure that it has all necessary and appropriate consents and notices in place to enable lawful transfer of the Personal Data to SW for the duration and purposes of the Agreement so that SW may lawfully use, process and transfer the Personal Data in accordance with the Agreement on

Customer's behalf. The Customer will not transfer any Personal Data to SW in connection with the provision of Services by SW, other than Personal Data of Candidates to the extent necessary for such Candidates to liaise with SW in respect of such Services.

4 DATA SUBJECT RIGHTS AND COOPERATION

4.1 SW shall notify Customer without undue delay if it receives a request from an individual attempting to exercise their rights under Data Protection Laws or any legally binding request for disclosure of a Candidate's Personal Data by a law enforcement authority or regulatory body unless such notification is unlawful.

4.2 SW will provide such reasonable assistance and information to the Customer as the Customer may reasonably require to allow the Customer to comply with their obligations under the Data Protection Laws, including assisting the Customer to:

4.2.1 respond to requests from individuals exercising their rights under Data Protection Laws (taking into account the nature of the processing undertaken by SW);

4.2.2 conduct a data protection impact assessment (and any related consultations) where required under Data Protection Laws (taking into account the nature of the processing undertaken by, and information available to, SW); and

4.2.3 report any Personal Data Breaches to the relevant Supervisory Authority and/or affected individuals.

5 CONFIDENTIALITY

5.1 SW shall ensure that:

5.1.1 any staff or personnel authorised to process the Personal Data are subject to a binding duty of confidentiality in respect of such data to requests from individuals exercising their rights under Data Protection Laws (taking into account the nature of the processing undertaken by SW);

5.1.2 access to such Personal Data under the Agreement is on a strictly need to know basis as necessary for staff or personnel to perform their roles in performance of this DPA;

5.1.3 any staff or personnel are appropriately reliable, qualified and trained in relation to their Processing of Personal Data.

6 SECURITY OF PROCESSING

6.1 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, SW will implement appropriate technical and organisational measures to protect Personal Data against a Personal Data Breach, including inter alia as appropriate:

6.1.1 the pseudonymisation and encryption of Customer Personal Data;

6.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.1.3 the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident;

6.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing; and

6.1.5 any other measures taken in accordance with Appendix 2 (TOMs).

6.2 SW shall notify Customer without undue delay, and in any event, no later than 24 hours, should it become aware of a Personal Data Breach leading to the accidental or unauthorised loss, alteration or disclosure of Personal Data.

7 SUB-PROCESSORS

7.1 Customer provides a general authorisation to SW to engage Sub-Processors to process Personal Data. SW shall provide Customer with a list of those Sub-Processors, as set out at the Sub-Processors page. SW shall give Customer prior notice of any intended addition to or replacement of those Sub-Processors. If Customer objects to that change, SW shall take steps to resolve any reasonable concerns raised by Customer and shall keep Customer informed of those steps. Prior to engagement of a Sub-Processor, SW shall carry out due diligence to ensure that sufficient guarantees to keep Personal Data secure are in place.

7.2 SW shall ensure that it has a written contract with any Sub-Processors it engages to process Personal Data. That contract must impose obligations on the Sub-Processor at least equivalent to those set out in this DPA. Prior to engagement of a Sub-Processor, SW shall carry out due diligence to ensure that sufficient guarantees to keep Personal Data secure are in place.

8 INTERNATIONAL TRANSFERS

8.1 The Customer consents hereby to the transfer of Personal Data outside the European Economic Area subject to the following conditions being fulfilled: a) SW has provided an adequate level of protection and appropriate safeguards in relation to such transfer in accordance with the Data Protection Laws; and b) the Data Subject has enforceable rights and effective legal remedies. If SW is using a Third Party Processor who will process Personal Data outside the European Economic Area, then SW shall, prior to making any restrict transfer, conduct a transfer risk assessment and shall implement appropriate mitigations to address any risks or issues identified in transfer risk assessment. Before making that restricted transfer, SW shall enter into a data processing agreement with the Third Party Processor setting out terms substantially the same as the International Transfer Clauses, under which SW shall be described as the data exporter and the Third Party Processor shall be described as the data importer.

9 AUDIT

9.1 At the request of Customer, SW shall make available to the Customer all information necessary to demonstrate SW's compliance with this DPA when processing Personal Data ("Documentary Evidence of Compliance"). SW shall allow for, and contribute to, audits conducted by the Customer, at the Customer's own cost (either itself or using a reputable auditor nominated by the Customer and approved by SW (such approval not to be unreasonably withheld). Such audit shall be conducted as provided in the Agreement.

10 LIABILITIES

10.1 Subject to the limitations and exclusions of liability set out in the Agreement, each Party undertakes to indemnify the other in respect of all liabilities, damages, losses, fines, claims, demands, expenses and costs (including reasonable legal fees) for any claim brought by or on behalf of a Data Subject that occurred due to the Customer and/or the Data Subject's failures to observe correct document upload processes and protocols as communicated by SW, and/or SW acting in accordance with any instruction, policy or procedure of Customer.

11 DATA RETENTION AND TERMINATION

11.1 Save as required by law and subject to earlier expiration or termination of this Agreement, SW shall destroy or delete all Candidates' Personal Data (including a Candidate's screening file) not later than 36 months from the last screening outcome ("Completed", "Failed", "Withdrawn") as such outcome is shown on the System. If the Customer requires with just cause that SW retains records for longer than 6 months, SW will charge additional charges for doing so in accordance with the Agreement and shall destroy or delete such Personal data following the lapse of such longer retention period requested by the Customer save as required by law.

11.2 On termination of the Agreement, and at the option of Customer, SW shall promptly return or delete Personal Data and certify in writing that it has done so. SW may retain a copy of Customer data where required by relevant law but must delete Customer data when that legal obligation ceases to apply. Notwithstanding the foregoing, SW shall only be required to use reasonable endeavours to delete copies of Personal Data held in backup or disaster recovery systems.

APPENDIX 1 – DATA PROCESSING PARTICULARS

Subject matter of the processing	Processing of Personal Data relating to the provision of employment screening services for Candidates put forward by the Customer as provided in the Agreement.
Duration of the processing / Retention of Personal Data	Personal Data will be processed for the term of the Agreement; Personal Data will be destroyed or deleted as per Clauses 11.1 and 11.2 of this DPA.
Nature and purpose of the processing	Purpose of the processing is the performance of SW's obligations under the Agreement,. The nature of the processing will include, as part of the provision of employment or pre-employment screening services under the Agreement, actions such as collection, storing, consulting, using, and deleting the Personal Data.
Type of Personal Data processed	Including but not limited to: Full name (including previous names and aliases), email address, date of birth, gender, current address and address history, place of birth, nationality, ID documentation (e.g., copy of passport, driving license, etc.), selfie image, activity history (employment, self-employment, education, gaps/periods of unemployment), job title and details of directorships, Right to Work information, National Insurance number, salary and transactional information, financial probity details such as CCJs, bankruptcy, etc and criminal offence data (if declared by candidate in online form).
Categories of Data Subjects	Candidates as such term is defined in the Agreement.
Obligations and rights of Customer	The obligations and rights of the Customer are set out in the Agreement.
Transfer of Personal Data outside the EEA	Clause 8.1 of this DPA shall apply.
Appointment of Sub-Processors	Clause 7.1 and 7.2 of this DPA shall apply. SW appoints the Sub-Processors set out at the Sub-Processors page.

APPENDIX 2 – TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

Domain	Practices
Information Security Policy and Organization of Information Security	**Ownership for Security and Data Protection**. Security Watchdog has appointed a Chief Risk & Assurance Officer, Information Security Manager and Data Privacy Officer responsible for coordinating and monitoring the security rules and procedures as well as data protection compliance. **Security Roles and Responsibilities**. Security responsibilities of Security Watchdog staff are formally documented and published in security and privacy policies. **Risk Management Program**. Security Watchdog executes periodical risk assessments of the implemented security controls.
Human Resources Security	**Confidentiality obligations**. Security Watchdog staff and contractors are subject to confidentiality obligations, and these are integrated into employment contracts/agreements. **Security and privacy training**. Security Watchdog informs its staff about relevant security measures to protect Customer Data. **Termination.** Security Watchdog ensures according to formal security administration procedures that access rights are timely revoked upon termination.
Asset Management	**Asset Inventory**. Security Watchdog maintains an inventory of all computing equipment and media used. Access to the inventories is restricted to authorized Security Watchdog personnel. **Asset Handling** - Data on portable devices are encrypted. - Security Watchdog has procedures for securely disposing of media and printed materials that contain confidential data.
Cryptography	Encryption of Customer Data is performed according to formal processes and encryption standards. SSL/TLS encryption mechanisms follow the highest standards only using strong ciphers and at least 256-bit encryption.
Physical and Environmental Security	**Physical Security of Facilities.** - Security Watchdog ensures physical security controls of its facilities and data centres are in place, including those managed by supplier. Including visitor management, secure entry, CCTV, and monitoring. **Physical Access to Facilities**. - Security Watchdog limits access to facilities to identified and authorized individuals. - Physical access to Security Watchdog premises and/or data centers is only granted following a formal authorization procedure and access rights are reviewed periodically. **Protection from Disruptions**. Security Watchdog uses a variety of industry standard systems to protect its data centers against loss of data due to power supply failure, fire and other natural hazards.

Domain	Practices
Access Control	**Access Policy**. Security Watchdog enforces an access control policy based on need-to-know and least privileges principles. **Access Authorization** - Security Watchdog has implemented and maintains an authorization management system that controls access to systems containing Customer Data. - Every individual accessing systems containing Customer Data has a separate, unique identifier/username. - Security Watchdog restricts access to Customer Data to those individuals who require such access to perform their job function. **Authentication** - Security Watchdog uses industry standard practices to identify and authenticate Users who attempt to access Security Watchdog network or information systems, including strong authentication. - Where Authentication Credentials are based on passwords, Security Watchdog requires that the passwords are at least eight characters long and sufficiently complex. - De-activated or expired identifiers/usernames are not granted to other individuals. - Accounts will be locked out in case of repeated attempts to gain access to the information system using an invalid password. - Security Watchdog maintains practices designed to ensure the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network access**. Security Watchdog maintains control measures (e.g. firewalls, security appliances, network segmentation) to provide reasonable assurance that access from and to its networks is appropriately controlled.
Operations Security	**Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a day (unless no data has been updated during that period), Security Watchdog maintains backup copies of Customer Data for recovery purposes. - Security Watchdog stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. **Malicious Software**. Security Watchdog maintains anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data. **Security updates**. Security patches are followed-up and installed following a documented security patch management process. **Event Logging**. Security Watchdog logs access and use of its information systems containing Customer Data, registering the access ID, time and relevant activity.
Communications Security	**Network Segregation**. Security Watchdog has implemented network segmentation controls to avoid individuals gaining access to communication and systems for which they have not been authorized. **Transfer outside own network**. Security Watchdog encrypts, or provides the mechanisms to the Customer to encrypt, customer information that is transferred across public networks. **Information Transfer**. Any transfer of Customer Data to third parties is only performed when authorized and following the execution of a formal written non-disclosure agreement.

Domain	Practices
System Acquisition, Development & Maintenance	**Security Requirements**. Requirements for protecting data and systems are analysed and specified. **Change Control**. Security Watchdog has implemented a formal change management process to ensure changes to operational systems and applications are performed in a controlled way.
Supplier Relationships	**Supplier Selection**. Security Watchdog maintains a selection process by which it evaluates the security and privacy and practices of a subcontractor with regard to data handling. **Contractual Obligations**. Suppliers with access to Customer Data are subject to data protection and security obligations and these are formally integrated into supplier contracts.
Information Security Incident Management	**Incident response**. Security Watchdog maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported. **Incident notification**. For each security breach that impact the confidentiality or integrity of Customer data, notification by Security Watchdog will be made without unreasonable delay.
Business Continuity Management	**Disaster Recovery**. Security Watchdog maintains a disaster recovery plan (DRP) for the facilities in which Security Watchdog information systems that process customer data are located. The DRP is tested at least annually. **Redundancy**. Security Watchdog' redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its last-replicated state from before the time it was lost or destroyed.
Compliance	**Security Reviews**. Information security controls are independently audited and reported to management on a periodical basis.