Last Updated: March 2026

This Data Protection Addendum ("**DPA**") forms part of the agreement ("**Agreement**") between the Sec Watchdog Limited, trading as Matrix MSW ("**MSW**") under which SW provides Customer (as defined in the Agreement and hereinafter "**Customer**") certain products or services ("**Services**") 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 MSW 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 MSW 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 MSW 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 MSW, it shall provide prior notice to Customer unless the relevant law prohibits the giving of notice on important grounds of public interest.

3.4 MSW 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 MSW for the duration and purposes of the Agreement so that MSW 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 MSW in connection with the provision of Services by MSW,

other than Personal Data of Candidates to the extent necessary for such Candidates to liaise with MSW in respect of such Services.

4 DATA SUBJECT RIGHTS AND COOPERATION

4.1 MSW 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 MSW 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 MSW), though for the avoidance of doubt, MSW is under no obligation to respond to the request on the Customer's behalf;

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, MSW); and

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

5 CONFIDENTIALITY

5.1 MSW 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 MSW);

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, MSW 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 MSW 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.

6.3 MSW 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 Customer's written consent, except when required to do so by law.

6.4 The Customer has the sole right to determine whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Information Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice.

7 SUB-PROCESSORS

7.1 Customer provides a general authorisation to MSW to engage Sub-Processors to process Personal Data. MSW shall provide Customer with a list of those Sub-Processors, as set out at the Sub-Processors page. MSW shall give Customer prior notice of any intended addition to or replacement of those Sub-Processors. If Customer objects to that change, MSW shall take steps to resolve any reasonable concerns raised by Customer and shall keep Customer informed of those steps.

7.2 MSW 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, MSW 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) MSW 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 MSW is using a Sub-Processor who will process Personal Data outside the European Economic Area, then MSW shall, prior to making any restricted 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, MSW shall enter into a data processing agreement with the Sub-Processor setting out terms substantially the same as the International Transfer Clauses, under which MSW shall be described as the data exporter and the Sub-Processor shall be described as the data importer.

9 AUDIT

9.1 The Customer may, upon giving no less than 30 days' written notice, request reasonable information and documentation from MSW to verify MSW's compliance with this DPA. MSW shall provide such information to the extent reasonably necessary and proportionate to the request. Audits shall be limited to once in any twelve (12) month period, unless the Customer has reasonable and evidencable suspicions that MSW has breached this DPA.

9.2 Any such audit shall be conducted during normal business hours and be carried out in a manner that minimises disruption to MSW's operation. Audits shall be limited to information directly relevant to MSW's obligations under this DPA. Under no circumstances shall the Customer be entitled to access:

9.2.1 Information relating to other customers of MSW;
9.2.2 MSW's internal security measures, infrastructure or system architecture; or
9.2.3 any trade secrets or commercially sensitive information.

9.3 MSW may satisfy audit requests by providing existing third-party certification and high-level summaries in place of direct access, where such materials reasonably demonstrate compliance.

9.4 The Customer shall bear its own costs in relation to any audit, unless the audit reveals a material breach of this DPA by MSW, in which case the reasonable and properly incurred costs of the audit shall be borne by MSW.

9.5 Where the Customer uses a third party to conduct the audit on its behalf, the Customer shall ensure that such third party is subject to appropriate confidentiality obligations no less than stringent than those set out 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 MSW, and/or MSW 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, MSW 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 MSW retains records for longer than 36 months, MSW 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 request of the Customer, MSW shall promptly return or delete Personal Data and certify in writing that it has done so. MSW 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, MSW 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 MSW'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. MSW appoints the Sub-Processors set out at the Sub-Processors page.

APPENDIX 2 – TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

Domain	Practices
Accreditations and Certifications	**ISO27001:2022.** MSW are accredited to ISO27001:2022 standard, we are audited and accredited by an independent UKAS accredited certification body, all controls are included in our Statement of Applicability, and our entire organisation is in scope of this accreditation. **Cyber Essentials and Cyber Essentials Plus.** MSW hold both Cyber Essentials and Cyber Essentials Plus certifications; our entire organisation is in scope of these certifications.
Information Security Policy and Organization of Information Security	**Ownership for Security and Data Protection**. MSW has appointed a Head of Infrastructure and Security, 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 MSW staff are formally documented and published in security and privacy policies. **Risk Management Program**. MSW conducts periodical risk assessments of the implemented security controls. An Information Security Risk Register is maintained by our Information Security Manager; regular reviews are conducted, risk and actions owners are assigned, and all actions are managed through to resolution.
Human Resources Security	**Confidentiality obligations**. MSW staff and contractors are subject to confidentiality obligations, and these are integrated into employment contracts/agreements. **Security and privacy training**. All MSW staff undergo a range of mandatory Information Security, Cyber Security Phishing and Data Protection training at least annually. **Termination.** MSW ensures according to formal security administration procedures that access rights are timely revoked upon termination.
Asset Management	**Asset Inventory**. MSW maintains an inventory of all computing equipment and media used. Access to the inventories is restricted to authorized MSW personnel. **Asset Disposal.** MSW has procedures for securely disposing of digital data, physical storage devices and printed materials that contain confidential data, certificates of destruction are provided post destruction by an independent third party.
Cryptography	**Encryption at rest.** All data is encrypted according to industry best practices using only strong encryption techniques, using

Domain	Practices
	AES-256 as a minimum. **Encryption in transit.** All data is encrypted in transit using highest standards (e.g. TLS 1.2, TLS 1.3) only using strong ciphers and at least 256-bit encryption.
Physical and Environmental Security	**Physical Security of Facilities.** MSW 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.** MSW limits access to facilities to identified and authorized individuals, physical access to MSW premises and/or data centres is only granted following a formal authorization procedure and access rights are reviewed periodically. **Protection from Disruptions.** MSW ensures appropriate controls are implemented to protect its data centres against data loss or system availability due to power supply failure, fire and other natural hazards.
Access Control	**Access Control Policy**. MSW enforces an access control policy strictly adhering to the principle of least privilege, and Role Based Access Controls (RBAC) is enforced across our estate.. **Access Authorization.** MSW has implemented and maintains an authorization management system that controls access to systems containing Customer Data. MSW restricts access to Customer Data to those individuals who require such access to perform their job function. **Authentication.** Every individual accessing systems containing Customer Data has a separate, unique identifier/username. Where Authentication Credentials are based on passwords, MSW requires that the passwords are at least 12 characters long, comprising of upper and lower case, numbers and special characters, with number matching MFA enabled for all user accounts. Administrator accounts require enhanced password standards and more frequent MFA authentication checks. Deactivated identifiers / usernames are not reused to other individuals. Accounts are locked out where case of repeated attempts to gain access using an invalid password are identified. Geo-location blocks on staff user access is in place to prevent access from non-UK locations. MSW maintains practices designed to ensure the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network access.** MSW maintains industry standard control measures (e.g. firewalls, security appliances, network segmentation) to ensure that access from and to its networks is appropriately controlled.

Domain	Practices
Operations Security	**Data Recovery Procedures.** On an ongoing basis, but in no case less frequently than once a day MSW maintains backup copies of Customer Data for recovery purposes. MSW stores copies of Customer Data and data recovery procedures in a geo-separate location from where the primary computer equipment processing the Customer Data is located. **Anti-Virus / Anti-Malware.** MSW maintains anti-virus and anti-malware controls to prevent malicious software gaining unauthorized access to Customer Data, virus definitions are updated automatically and protection cannot be disabled. **Security updates.** Security patches are identified, tested and installed following a documented security patch management process, distributed by our MDM solution, with forced updates and restarts to ensure all devices are compliant. **Event Logging**. MSW logs access and use of its information systems containing Customer Data, registering at a minimum, the access ID, time and relevant activity.
Communications Security	**Network Segregation**. MSW has implemented network segmentation controls to avoid individuals gaining access to communication and systems for which they have not been authorized. **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.
System Acquisition, Development & Maintenance	**Security Requirements**. Appropriate secure software development processes are in place including review of all changes, vulnerability and code scanning prior to deployment to ensure no vulnerabilities are introduced as a result of a change. **Change Control**. MSW 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**. MSW maintains a selection process by which it evaluates the security and privacy controls of a subcontractor, assessments are conducted by our Information Security Manager and Data Protection Officer prior to onboarding. Regular supplier security and data protections reviews are conducted to ensure continued compliance to our security standards. **Contractual Obligations**. Suppliers with access to Customer Data are subject to data protection and security obligations and these are formally integrated into supplier contracts.

Domain	Practices
Information Security Incident Management	**Incident response**. MSW maintains incident management processes, all security breaches are logged with a description of the breach, the time period, the consequences of the breach, the name of the reporter, to whom the breach was reported and root cause analysis **Incident notification**. Should a security or data breach occur which affects the Confidentiality, Integrity and/or Availability of client data, or our ability to provide services to our clients, we will notify clients in line with our contractual obligations and always without undue delay.
Business Continuity Management	**Disaster Recovery**. MSW maintains a business continuity and disaster recovery plans for our staff, offices and systems, these plans are tested at least annually. **Redundancy**. MSW maintains redundant and immutable backups and have comprehensive procedures for recovering data and systems.
Internal Compliance	**Internal Audits**. Internal audits are conducted across the business to ensure continued compliance with our security standards; any corrective actions identified are logged and managed through to resolution by our Information Security Manager.