

DATA PROCESSING AGREEMENT

This DPA is entered into between the Controller and the Processor and is incorporated into and governed by the provisions of the Agreement

1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement.

“Affiliate”	means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. “Control”, for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;
“Agreement”	means the agreement between the Controller and the Processor for the provision of the Service set out in more detail in the Terms;
“Controller”	means You;
“Customer Data”	means all data imported into the Service for the purpose of using the Service or facilitating use of the Service by You or your authorised users;
“Data Protection Law”	means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the UK GDPR, the UK Data Protection Act 2018, the FADP, US State Privacy Laws and any applicable national implementing laws, regulations and secondary legislation relating to the processing of the Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
“Data Subject”	shall have the same meaning as in Data Protection Law and includes a “Consumer” or “individual” as those terms are defined in US State Privacy Laws;
“DPA”	means this data processing agreement together with Exhibits A and B;
“EEA”	means the European Economic Area;
“EU GDPR”	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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);
“FADP”	means the Swiss Federal Act on Data Protection of the 1 st of September 2023, and as amended from time to time;
“Personal Data”	shall have the same meaning as in Data Protection Law and includes “personally identifiable information”, as that term is defined in US State Privacy Laws;
“Processor”	means Us, including as applicable any “Service Provider” as that term is defined in US State Privacy Laws;
“Restricted Transfer”	means: <ul style="list-style-type: none"> (i) where the EU GDPR applies, a transfer of Personal Data via the Service from the EEA either directly or via onward transfer, to any

country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and

(ii) where the UK GDPR applies, a transfer of Personal Data via the Service from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

(iii) a transfer of Personal Data via the Service from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission;

“Service”

means all services and software applications and solutions provided to the Controller by the Processor under and as described in the Agreement;

“SCCs”

means:

(i) where the EU GDPR applies, the standard 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 published at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN>, (“**EU SCCs**”); and

(ii) where the UK GDPR applies the international data transfer addendum to the EU SCCs adopted pursuant to Article 46(2)(c) of the UK GDPR and published at <https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf>, as may be amended or replaced, (“**UK SCCs**”); and

(iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority; (“**Swiss SCCs**”); as they may be amended, superseded or replaced from time to time.

“Sub-processor”

means any third party (including the Processor's Affiliates) engaged directly or indirectly by the Processor to process Personal Data under this DPA in the provision of the Service to the Controller;

“Supervisory Authority”

means a governmental or government chartered regulatory body having binding legal authority over a party;

“UK GDPR”

means the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018;

“US State Privacy Laws”

means the following US state data protection or privacy laws and regulations applicable to the party's Processing of Personal Data: California Consumer Privacy Act (**CCPA**) as amended by the California Privacy Rights Act (**CPRA**), Virginia Consumer Data Protection Act (**VCDPA**), Colorado Privacy Act (**CPA**), Connecticut Data Privacy Act (**CTDPA**), and Utah Consumer Privacy Act (**UCPA**) and the Connecticut Data Privacy Act (**CTDPA**), the Montana Consumer Data Privacy Act (**MCDPA**), Consumer Data Protection (**Iowa CDPA**), the Delaware Personal Data Privacy Act (**DPDPA**), the Nebraska Data Privacy Act (**NDPA**), the New Hampshire Expectation of Privacy Act (**NHPA**) and the New Jersey Act Concerning Online Services,

Consumers, and Personal Data (**NJDPA**), in each case as may be amended or superseded from time to time.

2. Purpose

- 2.1 The Processor has agreed to provide the Service to the Controller in accordance with the terms of the Agreement. In providing the Service, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. Scope

- 3.1 In providing the Service to the Controller pursuant to the terms of the Agreement, the Processor shall process Personal Data only to the extent necessary to provide the Service in accordance with the terms of the Agreement, this DPA and the Controller's instructions documented in the Agreement and this DPA, as updated from time to time.
- 3.2 The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the Processor who has access to Personal Data does not process Personal Data except on the instructions from the Controller, unless required to do so by any Data Protection Law.

4. Processor's Obligations

- 4.1 The Processor may collect, process or use Personal Data only within the scope of this DPA.
- 4.2 The Processor confirms that it shall process Personal Data on behalf of the Controller in accordance with the documented instructions of the Controller.
- 4.3 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach Data Protection Law.
- 4.4 The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.
- 4.5 The Processor shall implement appropriate technical and organisational measures to protect Personal Data, taking into account: (i) the state of the art; (ii) the costs of implementation; (iii) the nature, scope, context and purposes of processing; and (iv) the risk of varying likelihood and severity for the rights and freedoms of natural persons.
- 4.6 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
- 4.7 The technical and organisational measures detailed in Exhibit B shall at all times be adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA, provided such measures are at least equivalent to the technical and organisational measures set out in Exhibit B and appropriate pursuant to the Processor's obligations in clauses 4.5 and 4.6 above.

- 4.8 The Controller acknowledges and agrees that, in the course of providing the s to the Controller, it may be necessary for the Processor to access the Personal Data to respond to any technical problems or Controller queries and to ensure the proper working of the Service. All such access by the Processor will be limited to those purposes.
- 4.9 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.
- 4.10 The Processor confirms that it and/or its Affiliate(s) have appointed a data protection officer where such appointment is required by Data Protection Law. The appointed data protection officer may be contacted as set out in Exhibit A.
- 4.11 The Processor may not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for commercial purposes other than providing the Service under the terms of the Agreement; or (iii) retain, use, or disclose Personal Data outside of the terms of the Agreement.

5. Controller's Obligations

- 5.1 The Controller represents and warrants that: (i) it shall comply with this DPA and its obligations under Data Protection Law; (ii) it has obtained any, and all, permissions and authorisations necessary to permit the Processor and Sub-processors, to execute their rights or perform their obligations under this DPA; and (iii) all Affiliates of the Controller who use the Service shall comply with the obligations of the Controller set out in this DPA.
- 5.2 The Controller shall implement appropriate technical and organisational measures to protect Personal Data, taking into account: (i) the state of the art; (ii) the costs of implementation; (iii) the nature, scope, context and purposes of processing; and (iv) the risk of varying likelihood and severity for the rights and freedoms of natural persons.
- 5.3 The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
- 5.4 The Controller acknowledges and agrees that some instructions from the Controller including the Processor assisting with audits, inspections, DPIAs or providing any assistance under this DPA, may result in additional fees. In such case the Processor shall notify the Controller of its fees for providing such assistance in advance and shall be entitled to charge the Controller for its reasonable costs and expenses in providing such assistance, unless agreed otherwise in writing.

6. Sub-processors

- 6.1 The Controller agrees that the Processor may engage Sub-processors in connection with the provision of the Service.
- 6.2 All Sub-processors who process Personal Data in the provision of the Service to the Controller shall comply with the obligations of the Processor set out in this DPA.
- 6.3 The Controller authorises the Processor to use the Sub-processors included in the list of Sub-processors published at: <https://www.infovetted.com/hubfs/legal/Sub-processors.pdf> to process the Personal Data. During the term of this DPA, the Processor shall provide the Controller with 30 days prior notification, via email, of any changes to the list of Sub-processors

before authorising any new or replacement Sub-processor to process Personal Data in connection with provision of the Service.

- 6.4 The Controller may object to the use of a new or replacement Sub-processor, by notifying the Processor promptly in writing within fifteen (15) days after receipt of the Processor's notice. If the Controller objects to a new or replacement Sub-processor, the Controller may terminate the Agreement with respect to any part of the Service which cannot be provided by the Processor without the use of the new or replacement Sub-processor. The Processor will refund the Controller any prepaid fees covering the remainder of the term of the Agreement following the effective date of termination with respect to such terminated part of the Service.
- 6.5 All Sub-processors who process Personal Data shall comply with the obligations of the Processor set out in this DPA. The Processor shall prior to the relevant Sub-processor carrying out any processing activities in respect of the Personal Data: (i) appoint each Sub-processor under a written contract containing materially the same obligations to those of the Processor in this DPA enforceable by the Processor; and (ii) ensure each such Sub-processor complies with all such obligations.
- 6.6 The Controller agrees that the Processor and its Sub-processors may make Restricted Transfers of Personal Data for the purpose of providing the Service to the Controller in accordance with the Agreement. The Processor confirms that such Sub-processors: (i) are located in a third country or territory recognised by the EU Commission or a Supervisory Authority, as applicable, to have an adequate level of protection; or (ii) have entered into the applicable SCCs with the Processor; or (iii) have other legally recognised appropriate safeguards in place.

7. Restricted Transfers

- 7.1 The parties agree that, when a transfer of Personal Data occurs between the Controller and the Processor or from the Processor to a Sub-processor which is a Restricted Transfer, it shall be subject to the applicable SCCs.
- 7.2 The parties agree that the EU SCCs shall apply to Restricted Transfers from the EEA. The EU SCCs shall be deemed entered into (and incorporated into this DPA by reference) and completed as follows:
- (i) Module Two (Controller to Processor) shall apply where You are a Controller of Personal Data and We are processing Personal Data;
 - (ii) Module Three (Processor to Processor) shall apply where We are a Processor of Personal Data and We use a Sub-processor to process the Personal Data;
 - (iii) Module Four (Processor to Controller) shall apply where We are processing Personal Data and You are not subject to the EU GDPR or UK GDPR;
 - (iv) In Clause 7 of the EU SCCs, the optional docking clause shall not apply;
 - (v) In Clause 9 of the EU SCCs, Option 2 applies, and the time period for giving notice of Sub-processor changes shall be as set out in clause 6.3 of this DPA;
 - (vi) In Clause 11 of the EU SCCs, the optional language shall not apply;
 - (vii) In Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs shall be governed by Irish law;
 - (viii) In Clause 18(b) of the EU SCCs, disputes shall be resolved by the courts of Ireland;
 - (ix) Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A of this DPA;
 - (x) Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit B of this DPA.
- 7.3 The parties agree that the EU SCCs as amended in clause 7.2 above, shall be adjusted as set out below where the FADP applies to any Restricted Transfer:

- (i) The Swiss Federal Data Protection and Information Commissioner (“FDPIC”) shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the FADP;
 - (ii) Restricted Transfers subject to both the FADP and the EU GDPR, shall be dealt with by the EU Supervisory Authority named in Exhibit A of this DPA;
 - (iii) The term ‘member state’ must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;
 - (iv) Where Restricted Transfers are exclusively subject to the FADP, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP;
 - (v) Where Restricted Transfers are subject to both the FADP and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP insofar as the Restricted Transfers are subject to the FADP;
- 7.4 The parties agree that the UK SCCs shall apply to Restricted Transfers from the UK and the UK SCCs shall be deemed entered into (and incorporated into this DPA by reference), completed as follows:
- (i) Table 1 of the UK SCCs shall be deemed completed with the information set out in Exhibit A of this DPA;
 - (ii) Table 2 of the UK SCCs shall be deemed completed with the information set out in clauses 7.2(i) – (viii) of this DPA;
 - (iii) Table 3 of the UK SCCs shall be deemed completed with the information set out in Exhibits A and B of this DPA; and
 - (iv) Either party may end the UK SCCs as set out in clause 19 of the UK SCCs.
- 7.5 If changes are made to the EU SCCs or UK SCCs in the future, the parties shall negotiate in good faith necessary amendments to the DPA and the Agreement to ensure compliance with applicable Data Protection Law.
- 7.6 In the event that any provision of this DPA contradicts directly or indirectly any SCCs, the provisions of the applicable SCCs shall prevail over the terms of the DPA.
- 7.7 Should countries other than those in the EEA, UK or Switzerland adopt cross-border data transfer clauses similar to the SCCs, the Controller and Processor agree to execute such clauses when necessary.

8. Data Subject Access Requests

- 8.1 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Controller acknowledges and agrees that the Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.
- 8.2 In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.

9. Audit

- 9.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.
- 9.2 Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may conduct a

more extensive audit which shall be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance; (iii) carried out during the Processor's usual business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Processor's day-to-day business.

- 9.3 This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

10. Personal Data Breach

- 10.1 The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("**Personal Data Breach**").
- 10.2 In the event of a Personal Data Breach, the Processor shall take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Personal Data Breach, and to assist the Controller in meeting the Controller's obligations under applicable law.

11. Compliance, Cooperation and Response

- 11.1 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller, unless such notification is not permitted under applicable law or a relevant court order.
- 11.2 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.
- 11.3 The Processor shall reasonably assist the Controller in meeting the Controller's obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of the processing and the information available to the Processor.
- 11.4 The Controller shall notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the Processor is unable to accommodate necessary changes, the Controller may terminate the part or parts of the Service which give rise to the non-compliance. To the extent that other parts of the Service provided are not affected by such changes, the provision of that part of the Service shall remain unaffected.
- 11.5 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Law.

12. Liability

- 12.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.
- 12.2 The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.
- 12.3 The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Controller itself.
- 12.4 The Controller shall not be entitled to recover more than once in respect of the same loss.

13. Term and Termination

- 13.1 The Processor shall only process Personal Data for the term of the DPA. The term of this DPA shall commence on the Effective Date of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

14. Deletion and Return of Personal Data

- 14.1 The Processor shall at the choice of the Controller, upon receipt of a written request received within 30 days of the end of the provision of the Service, delete or return Personal Data to the Controller. The Processor shall in any event delete all copies of Personal Data in its systems within 180 days of the effective date of termination of the Agreement or deactivation of the Controller's account unless applicable law or regulations require storage of the Personal Data after termination.

15. General

- 15.1 This DPA sets out the entire understanding of the parties with regards to the subject matter herein.
- 15.2 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.
- 15.3 Subject to any provision of the SCCs to the contrary, this DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.
- 12.4 The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

Exhibit A

List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority

A. LIST OF PARTIES

The Exporter:

means You.	
Address:	As set out for You in the Agreement.
Contact person's name, position and contact details:	As provided by You in Your account and used for notification and invoicing purposes.
Activities relevant to the data transferred under the SCCs:	Use of the Service.
Signature and date:	By entering into the Agreement, the Exporter is deemed to have signed the SCCs incorporated into this DPA, including their Annexes, as of the start date of the Agreement.
Role:	Controller.
Name of Representative (if applicable):	Any UK or EU representative named in the Exporter's privacy policy.

The Importer:

means Info Vetted Limited	
Address:	10 Orange Street, London, WC2H 7DQ, England.
Contact person's name, position and contact details:	DPO, Luke Chittock, luke@infovetted.com
Activities relevant to the data transferred under the SCCs:	The provision of cloud computing solutions to the Exporter under which the Importer processes Personal Data upon the

	instructions of the Exporter in accordance with the terms of the Agreement.
Signature and date:	By entering into the Agreement, the Importer is deemed to have signed the SCCs, incorporated into this DPA, including their Annexes, as of the start date of the Agreement.
Role:	Processor.
Name of EU Representative (if applicable):	N/A

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of Data Subjects:	<p>Employees, agents, advisors, consultants, freelancers of the Controller (who are natural persons).</p> <p>Potential future employees (“Candidates”) of the Controller (who are natural persons) and individuals with whom those end users communicate with by email and/or other messaging media.</p> <p>Employers or persons providing references for Candidates.</p> <p>Users, Affiliates and other participants authorised by the Controller to access or use the Service in accordance with the terms of the Agreement.</p> <p>Other individuals to the extent identifiable in the context of emails of their attachments or in archiving content.</p> <p>Customers, prospective customers, suppliers, vendors, business partners, and other contacts of the Controller.</p> <p>External recruiters, agencies, or service providers engaged by the Controller in connection with candidate screening.</p> <p>Any other individuals whose personal data is submitted to, stored on, or transmitted through the Service.</p>
Categories of Personal Data:	<p>The Controller may submit Personal Data to the Service, the extent of which is determined and controlled by the Controller.</p> <p>The Personal Data includes but is not limited to:</p> <p>1. Customer Portal (Employers / Recruitment Agencies) The customer portal is used by employers or recruitment agencies or external HR management companies. Through this</p>

	<p>portal, they collect:</p> <ul style="list-style-type: none"> • Candidate details to initiate checks (name, email, date of birth, contact info, job role, job start date). <ul style="list-style-type: none"> ○ This could be synchronised through 3rd party tools such as Zapier/Knit ○ This could be synchronised directly via the HRIS/ATS provider • Employment information (e.g. role, start date, industry). • Supporting documents provided by the Controller (CVs, application forms, proof of right-to-work, proof of candidate Identification). • Instructions on which screening checks are to be performed. • Data from third parties such as DBS/police, credit reference agencies, educational institutions, previous employers/referees, Reed Screening Home Office (for right-to-work). <p>2. Candidate Portal (Applicants / Employees)</p> <p>The candidate portal is used directly by the individuals being screened. Through this portal, Controller collects:</p> <ul style="list-style-type: none"> • Identity information (name, date of birth, nationality, address history). • Contact details (email, phone, postal address). • Identity documents (passport, driving licence, visa, NI number). • Education and qualification details. • Employment history and referee details. • Professional Credentials, References, Character data, Online data. • Social media data (to the extent permitted by law).. • Declarations, consent forms, and questionnaires (e.g. for criminal record checks, financial checks, health declarations if required). • Uploaded supporting documents (scans, certificates, references). <p>In addition the following personal data is processed in both the Candidate Portal and the Customer Portal:</p> <ul style="list-style-type: none"> • Unique identifiers (e.g. username, account number, password). • IP address and geolocation data derived from IP. • Metadata (e.g. sender, recipient, date, time, subject), which may include Personal Data. • Financial data (where relevant to background or credit checks). • File attachments containing Personal Data. • Records of use of the Service, including logs, audit trails, and business intelligence information. • Personal Data contained within emails, messages, and communications processed through the Service. • Survey responses, feedback, and assessment data. • Information provided by users in support enquiries. • Other Personal Data submitted, uploaded, or otherwise made available by the Controller from time to time.
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Sensitive Data:	<p>Personal data transferred includes but is not limited to the following special categories of Personal Data:</p> <ul style="list-style-type: none"> • Personal Data revealing racial or ethnic origin • political opinions, • health information • Data relating to criminal convictions and offences (including results of background checks, police checks, and right-to-work checks). • Biometric data (e.g. photographs, scanned IDs, or facial images used for identification purposes).
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis for the duration of the Agreement.
Nature of the processing:	<p>Processing operations include but are not limited to:</p> <ul style="list-style-type: none"> • providing screening services to the Controller for their employees or Candidates to assist Controller in complying with its obligations to screen employees and Candidates in an employment context.
Purpose(s) of the data transfer and further processing:	Personal Data is transferred to sub-contractors who need to process some of the Personal Data in order to provide their services to the Processor as part of the Service provided by the Processor to the Controller.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	<p>Working copies of Customer Data will be securely deleted or anonymised within 30 – 90 days after the effective date of termination of the Agreement.</p> <p>Backup copies and archives of Customer Data will be securely overwritten as part of the backup cycle up to 180 days after the effective date of termination of the Agreement. During such 180 day period there is no active use of Customer Data.</p>
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Sub-processor list published at: Sub-Processor List sets out the Personal Data processed by each Sub-processor and the services provided by each Sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies (e.g. in	Where the EU GDPR applies, the Irish Data Protection Authority - Data Protection Commission, (DPC).
-----------------------------------------------------------	-----------------------------------------------------------------------------------------------------

accordance with Clause 13 of the SCCs)	<p>Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO).</p> <p>Where the FADP applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).</p>
----------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Exhibit B

Technical and Organisational Security Measures (Including Technical and Organisational Measures to Ensure the Security of Data)

Below is a description of the technical and organisational measures implemented by the Processor (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Where applicable this Exhibit B will serve as Annex II to the SCCs.

Measure	Description
Measures of pseudonymisation and encryption of Personal Data	<p>For the purpose of transfer control, Personal Data is encrypted in transit using industry-standard protocols (TLS). Remote access to company systems requires strong authentication, including multi-factor authentication (MFA). Company devices are secured with full-disk encryption to protect data at rest on endpoints. The encryption technologies used are evaluated against their protective purpose and updated in line with current industry best practices.</p> <p>The Processor protects Personal Data using industry-standard encryption technologies. In Azure, all data at rest is encrypted by default using AES-256, and all data in transit is protected with Transport Layer Security (TLS). Company devices that may access Personal Data use full-disk encryption, and remote access to company systems requires multi-factor authentication.</p> <p>Encryption keys are managed through Azure's Key Management Service (Azure Key Vault), which uses FIPS 140-2 validated cryptographic modules. Access to encryption keys and encrypted data is restricted to authorised personnel only, and all access is logged and monitored.</p> <p>Where feasible, Personal Data is pseudonymised or minimised so that individuals cannot be identified without additional information, which is stored separately under strict access controls.</p>
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	<p>Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance to the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person.</p>

	To maintain data access control, state of the art encryption technology is applied to the Personal Data itself where deemed appropriate to protect sensitive data based on risk.
Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident	<p>All our applications are built stateless by using ARM Templates (Azure Resource Manager Templates) and can be easily recreated in different geographical regions. Data is stored in triplicate across 2 data centres, with 2 separate cross connections. The data centres can be switched in the event of flooding, earthquake, fire or other physical destruction or power outage protect Personal Data against accidental destruction and loss.</p> <p>The Processor maintains redundancy throughout its IT infrastructure in order to minimize the lack of availability to or loss of data. Backups are maintained hourly and daily in accordance with our backup procedures. The Processor maintains a disaster recovery policy and at least once per calendar year practice executing the policy.</p>
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	The Processor conducts regular internal reviews of its security controls and leverages automated monitoring of its infrastructure 24/7. The Processor's security practices are informed by recognized industry frameworks, including the CIS Benchmarks (for system configuration hardening) and the NIST Cybersecurity Framework (for risk-based security management). In addition, the Processor engages an independent third party to conduct penetration testing and security assessments at least once per calendar year.
Measures for user identification and authorisation	Remote access to the data processing systems is only possible through the Processor's secure VPN tunnel. If the users first authenticate to the secure VPN tunnel, after successful authentication authorisation is executed by providing a unique user name and password to a centralised directory service. All access attempts, successful and unsuccessful are logged and monitored.
Measures for the protection of data during transmission	Data in transit is protected by Transport Layer Security ("TLS").
Measures for the protection of data during storage	<p>Personal Data is only retained internally, and on the third party data centre servers, which are covered by Microsoft certifications.</p> <p>The Controller's archived data is encrypted at rest using AES256 bit encryption and data in transit is protected by Transport Layer Security ("TLS").</p>

Measures for ensuring physical security of locations at which Personal Data are processed	<p>As the Processor primarily operates on a remote-first basis, employees access company systems and resources from secure home offices rather than dedicated business premises. Physical access to infrastructure used to provide the Service is managed by third-party data centre providers, who maintain industry-standard security controls, including 24/7 monitoring, access restrictions, and compliance with recognised data centre security certifications (such as ISO 27001).</p> <p>Access to the Processor's systems and data is restricted to authorised personnel only and protected through multi-factor authentication (MFA), role-based access controls, and encrypted connections. Any third-party service providers engaged by the Processor are required to maintain equivalent security standards.</p>
Measures for ensuring events logging	System inputs are recorded in the form of log files therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted.
Measures for ensuring system configuration, including default configuration	The Processor configures its systems in alignment with recognised industry security benchmarks (such as the CIS Benchmarks). Secure configuration baselines are applied and maintained using automated tools to ensure that systems do not deviate from the approved specifications. Detected deviations are automatically corrected where possible and logged for review by the Processor's security team.
Measures for internal IT and IT security governance and management	<p>Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems.</p> <p>The Controller's Personal Data is stored in a way that logically separates it from other customer data.</p>
Measures for certification/assurance of processes and products	The Processor is not currently ISO 27001 or ISO 27018 certified. However, the Processor has implemented and maintains a comprehensive Information Security Management System designed in alignment with industry best practices, including the principles of ISO 27001. The Processor applies documented technical and organisational security measures, which include (but are not limited to) regular risk assessments, access controls, encryption of data in transit and at rest, incident response procedures, and ongoing staff security training.

	<p>Upon the Controller's written request (no more than once in any 12-month period), the Processor shall provide, within a reasonable time, a summary of its current security policies, risk assessment outcomes, and evidence of relevant independent security testing (such as penetration tests or vulnerability assessments), to the extent that doing so does not prejudice the overall security of the Service. Any such information shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties.</p>
Measures for ensuring data minimisation	<p>If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.</p>
Measures for ensuring data quality	<p>All of the data that the Processor possesses is provided by the Controller. The Processor does not assess the quality of the data provided by the Controller. The Processor provides reporting tools within our product to help the Controller understand and validate the data that is stored.</p>
Measures for ensuring limited data retention	<p>The Processor uses a data classification scheme for all data that it stores and our retention policy specifies how each type of data is retained. When a record with Personal Data is deleted then it will be permanently evicted from our active databases. The data is retained in our backups until they are rotated out by more recent backups per the data retention policy.</p>
Measures for ensuring accountability	<p>The Processor internally reviews its information security policies semi-annually to ensure they it is still relevant and are being followed. All employees that handle sensitive data must acknowledge the information security policies. These employees are re-trained on information security policies once per year. A disciplinary policy is in place for employees that do not adhere to information security policies.</p>
Measures for allowing data portability and ensuring erasure	<p>The Service has built-in tools that allows the Controller to export and permanently erase data.</p>
Measures to be taken by the (Sub-) processor to be able to provide assistance to the Controller (and, for transfers from a Processor to a Sub-processor, to the Data Exporter).	<p>The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred outside the EEA, the Processor provides that an adequate level of data protection exists at the</p>

	target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the EU SCCs.
--	---------------------------------------------------------------------------------------------------------------------------------------------------------