

Centre for Assessment Ltd- ISO & EN1090 Audits

1. DATA PROTECTION

1.1 Each Party agrees to comply with its obligations as set out in Schedules 1A, 1B and 1C of this Agreement.

Schedule 1A

1. DEFINITIONS

In this Schedule 1A the following definitions shall apply:

"Applicable Law"	means the law of the United Kingdom;
"Controller", "Processor" and "Data Subject"	shall have the meaning given to those terms in the applicable Data Protection Laws;
"Data Protection Laws"	means (a) any law, statute, declaration, directive, regulation or other legislative enactment (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the GDPR and the UK GDPR and all legislation enacted in the UK in respect of the protection of personal data; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time;
"Data Processing Particulars"	means, in relation to any Processing under this Agreement: (a) the subject matter and duration of the Processing; (b) the nature and purpose of the Processing; (c) the type of Personal Data being Processed; and (d) the categories of Data Subjects; as set out in Schedule 1B.
"Data Subject Request"	means an actual or purported request from a Data Subject exercising his rights under the Data Protection Laws in relation to Personal Data including without limitation: the right of access by the Data Subject, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability and the right to object;
"GDPR"	means General Data Protection Regulation (EU) 2016/679;
"ICO"	means the UK Information Commissioner's Office, or any successor or replacement body from time to time;
"ICO Correspondence"	means any correspondence or communication (whether written or verbal) from the ICO in relation to the Processing of Personal Data;

Centre for Assessment Ltd- ISO & EN1090 Audits

"Losses"	means all losses, fines, penalties, liabilities, damages, costs, charges, claims, amounts paid in settlement and expenses (including legal fees (on a solicitor/client basis), disbursements, costs of investigation (including forensic investigation), litigation, settlement (including ex gratia payments), judgment, interest and penalties), other professional charges and expenses, disbursements, cost of breach notification including notifications to the data subject, cost of complaints handling (including providing data subjects with credit reference checks, setting up contact centres (e.g. call centres) and making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
"Permitted Recipients"	means the third parties to whom each Party is permitted to disclose the Personal Data, as set out in more detail in Schedule 1B (<i>Data Processing Particulars</i>);
"Personal Data"	means any personal data (as defined in the Data Protection Laws) Processed by either Party in connection with this Agreement, and for the purposes of this Agreement includes Sensitive Personal Data (as such Personal Data is more particularly described in Schedule 1B (<i>Data Processing Particulars</i>));
"Personal Data Breach"	has the meaning set out in the Data Protection Laws;
"Processing"	has the meaning set out in the Data Protection Laws (and " Process " and " Processed " shall be construed accordingly);
"Security Requirements"	means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws (including, in particular, the seventh data protection principle of the DPA and/ or the measures set out in Article 32(1) of the GDPR (taking due account of the matters described in Article 32(2) of the GDPR)) as applicable;
"Sensitive Personal Data"	means Personal Data that reveals such special categories of data as are listed in Article 9(1) of the GDPR;
"Third Party Request"	means a written request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law or regulation.
"UK GDPR"	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 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 of 2018.

Centre for Assessment Ltd- ISO & EN1090 Audits

2. DATA PROTECTION

2.1 Nature of the Processing

2.1.1 The Parties acknowledge that the factual arrangements between them dictate the role of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, each Party agrees that the nature of the Processing under this Agreement will be as follows:

- (a) the Parties shall each Process the Personal Data;
- (b) each Party shall act as a Controller in respect of the Processing of the Personal Data on its own behalf and in particular each shall be a Controller of the Personal Data acting individually and in common, as follows:
 - (i) Centre for Assessment Ltd shall be a Controller where it is Processing Personal Data in relation to the purpose described in Schedule 1B; and
 - (ii) the Client Organisation shall be a Controller where it is Processing Personal Data in relation to the purpose described in Schedule 1B;

Notwithstanding Paragraph 2.1.1(b), if either Party is deemed to be a joint Controller with the other in relation to the Personal Data, the Parties agree that they shall be jointly responsible for the compliance obligations imposed on a Controller by the Data Protection Laws, and the Parties shall cooperate to do all necessary things to enable performance of such compliance obligations, except that each Party shall be responsible, without limitation, for compliance with its data security obligations set out in Paragraph 2 where Personal Data has been transmitted by it, or while Personal Data is in its possession or control.

2.1.2 Each of the Parties acknowledges and agrees that Schedule 1B (*Data Processing Particulars*) to this Agreement is an accurate description of the Data Processing Particulars.

2.2 Data Controller Obligations

2.2.1 Each Party shall in relation to the Processing of the Personal Data comply with its respective obligations under the Data Protection Laws.

2.2.2 Without limiting the generality of the obligation set out in Paragraph 2.2.1, in particular, each Party shall:

- (a) where required to do so make due notification to the ICO;
- (b) ensure it is not subject to any prohibition or restriction which would:
 - (i) prevent or restrict it from disclosing or transferring the Personal Data to the other Party as required under this Agreement;
 - (ii) prevent or restrict it from granting the other Party access to the Personal Data as required under this Agreement; or

Centre for Assessment Ltd- ISO & EN1090 Audits

- (iii) prevent or restrict either Party from Processing the Personal Data, as envisaged under this Agreement;
- (c) ensure that all fair processing notices have been given (and/or, as applicable, consents obtained) and are sufficient in scope to enable each Party to Process the Personal Data as required in order to obtain the benefit of its rights and to fulfil its obligations under this Agreement in accordance with the Data Protection Laws;
- (d) ensure that all Personal Data disclosed or transferred to, or accessed by, the other Party is accurate, up-to-date and complete to enable either Party to Process the Personal Data as envisaged under this Agreement;
- (e) ensure that appropriate technical and organisational security measures are in place sufficient to comply with:
 - (i) at least the obligations imposed on the Controller by the Security Requirements; and
- (f) notify the other Party promptly, and in any event within forty-eight (48) hours of receipt of any Data Subject Request or ICO Correspondence which relates directly or indirectly to the Processing of Personal Data under, or in connection with, this Agreement and together with such notice, provide a copy of such Data Subject Request or ICO Correspondence to the other Party and reasonable details of the circumstances giving rise to it. In addition to providing the notice referred to in this Paragraph 2.2.2 (f), each Party shall provide the other Party with all reasonable co-operation and assistance required by the other Party in relation to any such Data Subject Request or ICO Correspondence;
- (g) use reasonable endeavours to notify the other Party if it is obliged to make a disclosure of any of the Personal Data under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless prohibited by law;
- (h) notify the other Party in writing without undue delay and, in any event, within twenty-four (24) hours of it becoming aware of any actual or suspected Personal Data Breach in relation to the Personal Data received from the other Party and shall, within such timescale to be agreed by the Parties (acting reasonably and in good faith):
 - (i) implement any measures necessary to restore the security of compromised Personal Data; and
 - (ii) support the other Party to make any required notifications to the ICO and/or other equivalent relevant Regulator and affected Data Subjects;
- (i) take reasonable steps to ensure the reliability of any of its personnel who have access to the Personal Data;
- (j) not do anything which shall damage the reputation of the other Party or that Party's relationship with the Data Subjects;

Centre for Assessment Ltd- ISO & EN1090 Audits

- (k) not transfer or otherwise process (and not instruct or permit a third party to transfer or otherwise process) Personal Data outside of the UK;
- (l) hold the information contained in the Personal Data confidentially and under at least the conditions of confidence as such Party holds Personal Data Processed by it other than the Personal Data;
- (m) not disclose the Personal Data to a third party (including a sub-contractor) in any circumstances without the other Party's prior written consent, save in relation to: (i) disclosures to Permitted Recipients; and (ii) Third Party Requests. For Third Party Requests, the Party seeking to disclose the Personal Data shall use reasonable endeavours to advise the other Party in advance of such disclosure, unless that Party is prohibited by law or regulation from notifying the other Party of that disclosure, in which case it shall do so as soon as practicable thereafter (where permitted by law or regulation); and
- (n) unless: either Party is required by Applicable Law or a regulatory body to retain the Personal Data at the other Party's option or direction, arrange for the prompt and safe return and/or secure permanent destruction of all Personal Data, together with all copies in its possession or control within 40 days and, where requested by the other Party certify that such destruction has taken place.

3. INDEMNITY

3.1 Both Parties shall indemnify on demand and keep indemnified the other Party from and against all and any Losses that are sustained, suffered or incurred by, awarded against or agreed to be paid by the other Party to the extent arising from the first Party's breach of its obligations under this Schedule 1A (Data Protection) and/or failure to comply with the Data Protection Laws, including, in particular all Losses resulting from:

- 3.1.1 any monetary penalties or fines levied by the ICO on the other Party;
- 3.1.2 the costs of an investigative, corrective or compensatory action required by the ICO, or the defence of a proposed or actual enforcement taken by the ICO;
- 3.1.3 any Losses suffered or incurred by, awarded against, or agreed to be paid by the other Party pursuant to a claim, action or challenge made by a third party to or against the other Party (including by a Data Subject); and
- 3.1.4 except to the extent covered by Paragraphs 3.1.1 or 3.1.2 or 3.1.3, any Losses suffered or incurred, awarded against or agreed to be paid by the other Party.

3.2 Growth Co's total liability to the Partner under clause 3.1 shall be limited to £100,000.

3.3 Nothing in this Agreement shall exclude or limit the Partner's liability under this Paragraph 3.

Centre for Assessment Ltd- ISO & EN1090 Audits

INSURANCE

Both Parties agree:

- 3.3.1 to obtain and keep in full force and effect at all times, in respect of the Processing of the Personal Data, a policy or policies of insurance covering legal liability arising to persons as a result of the Party's breach of this Schedule 1A (Data Protection) and/or failure to comply with the Data Protection Laws and to cover all liabilities under this Agreement:
- (a) it must cover legal liability arising to any person;
 - (b) it must apply in relation to the Processing of Personal Data;
- 3.3.2 to deliver to the other Party upon request:
- (a) copies of all applicable insurance policies taken out pursuant to the provisions of this Agreement;
 - (b) evidence of premiums paid in relation to such insurance.

Schedule 1B

Data Protection Particulars

The subject matter of the Processing	The delivery of audits and assessments to the applicable ISO or EN1090 standard
The nature of the Processing	<p>Obtaining, recording, and retaining staff contact details to plan and carry out the assessment contract.</p> <p>The personal data will be transmitted by the firm/organisation application forms and email to auditors</p> <p>Sharing personal data with awarding bodies and auditors includes name & contact details</p>
The duration of the Processing	10 Years
The purpose of the Processing	<p>To audit the Client Organisation to check compliance against the applicable ISO/EN1090 standard</p> <p>To be able to comply with UKAS accreditation and certification requirements for the applicable ISO/EN1090 standard.</p> <p>The audit reports which may contain personal data which has been collected for the purpose of auditing</p>

Centre for Assessment Ltd- ISO & EN1090 Audits

	compliance the applicable standard may be shared with UKAS for the purpose of accreditation requirements of a UKAS certification body.
The type of Personal Data being Processed	Name, contact details, qualifications, employment details
The categories of Data Subjects	Organisations staff and clients