Data Processing Agreement

disclosure services

Expert Support. Informed Clients. Clear Decisions.

BETWEEN:

(1) The client named on the 'registration form' under 'organisation name' and 'primary address' ("Data Controller") and;

(2) Disclosure Services Ltd a company registered in England & Wales under number 04198359 whose registered office is at Ellice House, Ellice Way Wrexham Technology Park Wrexham LL13 7YL ("Data Processor")

WHEREAS:

(1) Under a written agreement between the Data Controller and the Data Processor ("the Service Agreement") the Data Controller from time to time engages the Data Processor to provide to the Data Controller the Services described in Schedule 1.

(2) The provision of the Services by the Data Processor involves processing the Personal Data on behalf of the Data Controller and the Data Subject.

(3) The Data Controller is required to have in place an agreement in writing between the Data Controller and any organisation which processes personal data on its behalf governing the processing of that data. This is that agreement for the services described in Schedule 1.

(4) The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the GDPR (General Data Protection Regulation) and DPA (Data Protection Act 2018) in relation to all processing of the Personal Data by the Data Processor for the Data Controller and Data Subject.

(5) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Data Controller and Data Subject by the Data Processor and to all Personal Data held by the Data Processor in relation to all such processing.

IT IS AGREED as follows:

1. **Definitions and Interpretation**

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Data Controller", "Data Processor", "processing", and "data subject"	shall have the meanings given to the terms "controller", "processor", "processing", and "data subject" respectively in Article 4 of the GDPR;
"ICO"	means the UK's supervisory authority, the Information Commissioner's Office;
"Personal Data"	means all such "personal data", as defined in Article 4 of the GDPR, as is, or is to be, processed by the Data Processor on behalf of the Data Controller and Data Subject.

“Services”	means those services described in Schedule 1 which are provided by the Data Processor to the Data Controller and Data Subject and which the Data Controller uses for the purpose described in Schedule 1;

1.2 Unless the context otherwise requires, each reference in this Agreement to:

1.2.1 “writing”, and any similar expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;

1.2.2 a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

1.2.3 “this Agreement” is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

1.2.4 a Schedule is a schedule to this Agreement; and

1.2.5 a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule.

1.2.6 a "Party" or the "Parties" refer to the parties to this Agreement.

1.3 The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.4 Words imparting the singular number shall include the plural and vice versa.

1.5 References to any gender shall include all other genders.

1.6 References to persons shall include corporations.

2. Scope and Application of this Agreement

2.1 The provisions of this Agreement shall apply to the processing of the Personal Data, carried out for the Data Controller by the Data Processor, and to all Personal Data held by the Data Processor in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.

2.2 The provisions of this Agreement supersede any other arrangement, understanding, or agreement including, but not limited to, the Service Agreement made between the Parties at any time relating to the Personal Data.

2.3 This Agreement shall continue in full force and effect for so long as the Data Processor is processing Personal Data on behalf of the Data Controller, and thereafter as provided in Clause 9.

3. Provision of the Services and Processing Personal Data

The Data Processor is only to carry out the Services, and only to process the Personal Data received from the Data Controller:

3.1 for the purposes of those Services and not for any other purpose;

3.2 to the extent and in such a manner as is necessary for those purposes; and

3.3 strictly in accordance with the express written authorisation and instructions of

the Data Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Data Controller to the Data Processor).

4. **Data Protection Compliance**

4.1 All instructions given by the Data Controller to the Data Processor shall be made in writing and shall at all times be in compliance with the GDPR, DPA and other applicable laws. The Data Processor shall act only on such written instructions from the Data Controller unless the Data Processor is required by law to do otherwise (as per Article 29 of the GDPR).

4.2 The Data Processor shall promptly comply with any request from the Data Controller or Data Subject requiring the Data Processor to amend, transfer, delete, or otherwise dispose of the Personal Data for each applicant.

4.3 The Data Processor shall transfer all Personal Data to the Data Controller on the Data Controller's request in the formats, at the times, and in compliance with the Data Controller's written instructions.

4.4 Both Parties shall comply at all times with the GDPR, DPA and other applicable laws and shall not perform their obligations under this Agreement or any other agreement or arrangement between themselves in such way as to cause either Party to breach any of its applicable obligations under the GDPR.

4.5 The Data Controller hereby warrants, represents, and undertakes that the Personal Data shall comply with the GDPR & DPA in all respects including, but not limited to, its collection, holding, and processing.

4.6 The Data Processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with any and all applicable legislation from time to time in force (including, but not limited to, the GDPR) and any best practice guidance issued by the ICO.

4.7 The Data Processor shall provide all reasonable assistance to the Data Controller in complying with its obligations under the GDPR with respect to the security of processing, the notification of personal data breaches, the conduct of data protection impact assessments, and in dealings with the ICO.

4.8 When processing the Personal Data on behalf of the Data Controller, the Data Processor shall:

4.8.1 not process the Personal Data outside of the United Kingdom without the prior consent of the Data Controller. See also schedule 1.

4.8.2 not transfer any of the Personal Data (except those listed in Schedule 1) to any third party without the written consent of the Data Controller and, in the event of such consent, the Personal Data shall be transferred strictly subject to the terms of a suitable agreement, as set out in Clause 10;

4.8.3 process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Data Controller or as may be required by law (in which case, the Data Processor shall inform the Data Controller of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law);

4.8.4 implement appropriate technical and organisational measures, as described in Schedule 2, and take all steps necessary to protect the Personal Data against unauthorised or unlawful processing, accidental loss, destruction, damage, alteration, or disclosure.

4.8.5 if so requested by the Data Controller (and within the timescales required by the Data Controller) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;

4.8.6 keep detailed records of all processing activities carried out on the Personal Data.

4.8.7 make available to the Data Controller any and all such information as is reasonably required and necessary to demonstrate the Data Processor's compliance with the GDPR;

4.8.8 on at least 30 working days' prior notice, submit to audits and inspections and provide the Data Controller with any information reasonably required in order to assess and verify compliance with the provisions of this Agreement and both Parties' compliance with the requirements of the GDPR.

4.8.9 inform the Data Controller immediately if it is asked to do anything that infringes the GDPR & DPA or any other applicable data protection legislation.

5. Data Subject Access, Complaints, and Breaches

5.1 The Data Processor shall assist the Data Controller or Data Subject in complying with its obligations under the GDPR & DPA. In particular, the following shall apply to data subject access requests, complaints, and data breaches.

5.2 The Data Processor shall cooperate fully with the Data Controller or Data Subject and assist as required in relation to any subject access request, complaint, or other request that involves the Data Controller, including by:

5.2.1 providing the Data Controller with full details of the complaint or request;

5.2.2 providing the necessary information and assistance in order to comply with a subject access request;

5.2.3 providing the Data Controller or Data Subject with any Personal Data it holds in relation to a data subject (within 30 days notice); and

5.2.4 providing the Data Controller with any other information requested by the Data Controller.

5.3 The Data Processor shall notify the Data Controller if it becomes aware of any form of Personal Data breach involving the Data Controller or Data Subject, including any unauthorised or unlawful processing, loss of, damage to, or destruction of any of the Personal Data.

6. Appointment of a Data Protection Officer

6.1 The Data Processor has appointed a Data Protection Officer in accordance

with the GDPR, whose details are as follows: Steven Burgess | +44 (0)1978 510100 | www.disclosureservices.com | steven.burgess@disclosureservices.com

6.2 Ellice House, Ellice Way, Yale Business Village, Wrexham, LL13 7YL

7. Liability and Indemnity

7.1 The Data Controller shall be liable for, and shall indemnify (and keep indemnified) the Data Processor in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Data Processor and any Sub-Processor i.e. the Disclosure and Barring Service, Disclosure Scotland, Access Northern Ireland arising directly or in connection with:

7.1.1 any non-compliance by the Data Controller with the GDPR or other applicable legislation;

7.1.2 any Personal Data processing carried out by the Data Processor or Sub-Processor in accordance with instructions given by the Data Controller that infringe the GDPR or other applicable legislation; or

7.1.3 any breach by the Data Controller of its obligations under this Agreement,

except to the extent that the Data Processor or Sub-Processor is liable under sub-Clause 7.2.

7.2 The Data Processor shall be liable for, and shall indemnify (and keep indemnified) the Data Controller in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Data Controller arising directly or in connection with the Data Processor's Personal Data processing activities that are subject to this Agreement:

7.2.1 only to the extent that the same results from the Data Processor's or a Sub-Processor's breach of this Agreement; and

7.2.2 not to the extent that the same is or are contributed to by any breach of this Agreement by the Data Controller.

7.3 The Data Controller shall not be entitled to claim back from the Data Processor any sums paid in compensation by the Data Controller in respect of any damage to the extent that the Data Controller is liable to indemnify the Data Processor under sub-Clause 7.1.

7.4 Nothing in this Agreement (and in particular, this Clause 7) shall relieve either Party of, or otherwise affect, the liability of either Party to any data subject, or for any other breach of that Party's direct obligations under the GDPR. Furthermore, the Data Processor hereby acknowledges that it shall remain subject to the authority of the ICO and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a data processor under the GDPR may render it subject to the fines, penalties, and compensation requirements set out in the GDPR.

8. **Intellectual Property Rights**

All copyright, database rights, and other intellectual property rights subsisting in the Personal Data (including but not limited to any updates, amendments, or adaptations to the Personal Data made by either the Data Controller, Data Subject or the Data Processor) shall belong to the Data Controller or to any other applicable third party from whom the Data Controller has obtained the Personal Data under licence (including, but not limited to, data subjects, where applicable). The Data Processor is licensed to use such Personal Data under such rights only for the purposes of the Services, and in accordance with this Agreement.

9. **Confidentiality**

9.1 The Data Processor shall maintain the Personal Data in confidence, and in particular, unless the Data Subject has given written consent for the Data Processor to do so, the Data Processor shall not disclose any Personal Data supplied to the Data Processor by, for, or on behalf of, the Data Controller to any third party apart from those listed in Schedule 1. The Data Processor shall not process or make any use of any Personal Data supplied to it by the Data Controller otherwise than in connection with the provision of the Services to the Data Controller.

9.2 The Data Processor shall ensure that all personnel who are to access and/or process any of the Personal Data are contractually obliged to keep the Personal Data confidential.

9.3 The obligations set out in in this Clause 9 shall continue for a period of twelve months after the cessation of the provision of Services by the Data Processor to the Data Controller.

9.4 Nothing in this Agreement shall prevent either Party from complying with any requirement to disclose Personal Data where such disclosure is required by law. In such cases, the Party required to disclose shall notify the other Party of the disclosure requirements prior to disclosure, unless such notification is prohibited by law.

10. **Appointment of Sub-Processors**

10.1 The Data Processor and data processing involves the sub-processors listed in Schedule 1 of this agreement.

11. **Deletion and/or Disposal of Personal Data**

11.1 The Data Processor shall, at the written request of the Data Controller or Data Subject, delete (or otherwise dispose of) the Personal Data within a reasonable time after the earlier of the following:

11.1.1 the end of the provision of the Services;

11.2 Following the deletion, disposal, or return of the Personal Data under sub-Clause 11.1, the Data Processor shall delete (or otherwise dispose of) all further copies of the Personal Data that it holds, unless retention of such copies is required by law, in which case the Data Processor shall inform the Data Controller of such requirement(s) in writing.

11.3 All Personal Data to be deleted or disposed of under this Agreement shall be deleted or disposed of using the following method(s): electronic deletion or

shredding.

12. **Law and Jurisdiction**

12.1 This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

12.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

SCHEDULE 1

Services and sub-processors

1. Through the Disclosure and Barring Service (DBS) - Enhanced, Standard and Basic level criminal record disclosures.

2. Through Disclosure Scotland - Protected Vulnerable Groups Scheme (PVG) Membership and Scheme Update applications, Enhanced, Standard and Basic level criminal record disclosures.

3. Through Access Northern Ireland (ANI) – Enhanced and Standard level criminal record disclosures.

4. Through Amazon Web Services, London UK. Application data relating to point 1 and point 2 (Scottish Basics only) of this Schedule 1.

5. Back up through Amazon Web Services, Dublin (EU). Application data relating to point 1 and point 2 (Scottish Basics only) of this Schedule 1.

SCHEDULE 2

Technical and Organisational Data Protection Measures

The following are the technical and organisational data protection measures referred to in Clause 4:

1. The Data Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Data Controller, it maintains security measures to a standard appropriate to:

   1.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data; and

   1.2 the nature of the Personal Data.

2. In particular, the Data Processor shall:

   2.1 have in place, and comply with, a security policy which:

      2.1.1 defines security needs based on a risk assessment;

      2.1.2 allocates responsibility for implementing the policy to a specific individual (such as the Data Processor's Data Protection Officer) or personnel;

      2.1.3 is disseminated to all relevant staff; and

      2.1.4 provides a mechanism for feedback and review.

   2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

   2.3 prevent unauthorised access to the Personal Data;

   2.4 protect the Personal Data using pseudonymisation, where it is practical to do so;

   2.5 ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

   2.6 have secure methods in place for the transfer of Personal Data whether in physical or electronic form (for example, by using encryption);

   2.7 password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure, and that passwords are not shared under any circumstances;

   2.8 take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;

   2.9 have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:

      2.9.1 the ability to identify which individuals have worked with specific Personal Data;

      2.9.2 having a proper procedure in place for investigating and remedying breaches of the GDPR & DPA; and

2.9.3 notifying the Data Controller as soon as any such security breach occurs, if it involves the Data Controller's or Data Subject's data.

2.10 have a secure procedure for backing up all electronic Personal Data and storing back-ups separately from originals;

2.11 have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment; and

2.12 adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001, as appropriate to the Services provided to the Data Controller.