Data Processing Addendum

Definitions

1.1 In this agreement, unless the text specifically notes otherwise, the following definitions have the meanings given below:

Consent	is as defined in the Data Protection Laws
Contract	means the APCS Service Agreement
Controller	Is the Data Controller for this project, which is the customer for the services provided by the Processor as defined in the Contract
Data Protection Laws	is the UK Data Protection Legislation and EU Data Protection Legislation and any other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications)
UK Data Protection Legislation	is The UK GDPR as defined in The Data Protection Act 2018 Section 3(10), The Data Protection Act 2018, the Privacy & Electronic Communications (EC Directive) Regulations 2003 and any other applicable UK laws or replacement legislation coming into effect from time to time
EU Data Protection Legislation	is the GDPR - The General Data Protection Regulation (Regulation (EU) 2016/679) and any other applicable EU laws or replacement legislation coming into effect from time to time
Personal Data	is as defined in the Data Protection Laws
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed
Processing, processes, process	means any activity that involves the use of Personal Data or as the Data Protection Laws may otherwise define processing, processes or process. It includes any operation or set of operations which is performed on Personal Data or on sets of Personal Data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure

	or destruction. Processing also includes transferring Personal Data to a third party
Processor	is the Data Processor for this project, which is **Access Personal Checking Services Ltd., Enterprise House, The Courtyard, Old Court House Road, Bromborough, Wirral, CH62 4UE, United Kingdom, company registration number 07399692**
Services	the services set out in Schedule 1 and the Contract
Sub-Processor	means another processor engaged by the processor for carrying out processing activities in relation to this agreement
Supervisory Authority	means the Information Commissioner's Office (ICO) in the United Kingdom, or the local supervisory authority within the EU or EEA member state of the Controller

Terms of Agreement

2.1 The parties agree the above definitions of Controller and Processor and accept the roles described.

2.2 All processing of personal data by the Processor on behalf of the Controller shall be governed by this agreement and the terms obligations and rights set forth in this agreement relate directly to the data processing activities described in Schedule 1.

Obligations and Rights of the Processor

3.1 The Processor shall comply with the Data Protection Laws at all times and must:

a) only process the Personal Data to the extent, and in such a manner, as is necessary for the Provision of the Services in accordance with the Controller's written instructions. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Laws;
b) promptly notify the Controller if, in its opinion, the Controller's instruction would not comply with the Data Protection Laws;
c) maintain the confidentiality of all Personal Data and not disclose Personal Data to third parties unless the Controller specifically authorises the disclosure, or as required by law. If a law, court, regulator or Supervisory Authority requires the Processor to process or disclose Personal Data, the Processor must first inform the Controller of the legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice;
d) ensure that any people or Sub-Processors processing the Personal Data are subject to a duty of confidentiality and that such persons comply at all times with the terms of this Agreement;

e) Ensure that any natural person acting under their authority who has access to personal data does not process that data except on written instructions from the Controller;
f) Use its best endeavours to safeguard and protect all Personal Data from unauthorised or unlawful processing including but not limited to accidental loss destruction or damage and will ensure the security of processing through the demonstration and implementation of appropriate technical and organisational measures as specified in Schedule 1 of this agreement;
g) Ensure all processing meets the requirements of applicable Data Protection Laws;
h) Ensure that where a Sub-Processor is used, the Processor shall:
    I. Only engage a Sub-Processor with the agreement of the Controller;
    II. Inform the Controller of any intended changes regarding the addition or replacement of Sub-Processors listed in Schedule 1;
    III. Implement a written contract containing the same data protection obligations as set out in this agreement in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Data Protection Laws;
    IV. Remain fully liable to the Controller for the performance of the Sub-Processor's obligations in the event the Sub-Processor fails to comply with Data Protection Laws or relevant data processing agreement.
i) The Controller gives the Processor general authorisation to utilise Sub-Processors that provide general information technology and technical support including data storage and transmission services provided that obligations equivalent to the obligations set out in this clause 3 are included in all contract(s) between the Processor and the permitted Sub-Processors who will be processing Personal Data;
j) Assist the Controller in providing subject access and allowing Data Subjects to exercise their rights under the Data Protection Laws insofar as the Processor holds Personal Data relating to the Data Subjects;
k) Assist the Controller in meeting its data protection obligations in relation to:
    I. The security of processing by the Processor;
    II. Data Protection Impact Assessments for the provision of this service;
    III. The investigation and notification of personal data breaches caused by the Processor's Processing; and
l) Delete or return all personal data to the Controller as requested at the end of the agreement, or at such other time as the Controller may request;
m) Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the Data Protection Laws and allow for and contribute to one audit annually conducted by the Controller at the Controller's cost;
n) Cooperate with the Supervisory Authority in accordance with the Data Protection Laws;
o) Notify the Controller of any personal data breaches as soon as reasonably possible and in accordance with the Data Protection Laws.

3.2 Nothing within this agreement relieves the Processor of their own direct responsibilities obligations and liabilities under the Data Protection Laws.

3.3 The Processor is responsible for ensuring that each of its employees, agents, subcontractors or vendors are made aware of its obligations regarding the security and protection of the personal data and terms set out in this agreement.

3.4 The Processor shall maintain induction and training programmes that adequately reflect the Data Protection Law requirements and ensure that all employees are afforded the time resources and budget to undertake such training on a regular basis.

3.5 Any transfers of personal data to a third country or an international organisation shall only be carried out on written instructions from the controller unless required to do so by law and where such a legal requirement exists the Processor will inform the Controller of that legal requirement before processing.

3.6 Where required under the Data Protection Laws the Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller containing:

a) The name and contact details of the Processor and of each Controller on behalf of which the Processor is acting and where applicable the Data Protection Officer;
b) The categories of processing carried out on behalf of each Controller;
c) Transfers of personal data to a third country or an international organisation including the identification of that third country or international organisation and the documentation of suitable safeguards;
d) A general description of the technical and organisational security measures referred to in the Data Protection Laws.

3.7 When assessing the appropriate level of security and the subsequent technical and organisational measures, the Processor shall consider the risks presented by any processing activities, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosures of, or access to, personal data transmitted, stored, or otherwise processed.

Obligations and Rights of the Controller

4.1 The Controller is responsible for determining the means and purpose of processing and the lawful basis for processing and for meeting its obligations to the data subjects under the Data Protection Laws including providing the data subjects with an appropriate privacy notice.

4.2 The Controller reserves the right to verify that the Processor has adequate and documented processes for data breaches, data retention, and data transfers in place.

4.3 The Controller reserves the right to obtain evidence from the Processor as to the:

a) Verification and reliability of the employees used by the Processor;
b) Technical and organisational measures described in Schedule 1 of this agreement;
c) Procedures in place for allowing data subjects whose data are Processed under this agreement to exercise their rights in accordance with the Data Protection Laws.

4.4 Where the Controller has authorised the use of any Sub-Processors by the Processor the Controller may verify that similar data protection agreements are in place between the Processor and Sub-Processor.

Warranties

5.1 The Processor warrants and represents that:

a) its employees, subcontractors, agents and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Laws relating to the Personal Data;
b) it has no reason to believe that the Data Protection Laws prevent it from providing any of the Services; and

c) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:
   I. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;
   II. the nature of the Personal Data protected; and
   III. comply with all applicable Data Protection Laws.

Termination

6.1 This Agreement shall remain in full force and effect for so long as the Processor is providing the Services or the Processor retains Personal Data on behalf of the Controller.

6.2 The Processor's failure to comply with any of its obligations in clause 3 of this Agreement or if any of the warranties in clause 5 are found to be untrue or misleading then this shall be considered a material breach and the Controller may terminate effective immediately without further liability or obligation.

Governing Law

7.1 This Agreement is governed by the laws of England and Wales.

7.2 This Agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) is governed by and shall be construed and interpreted in accordance with the laws of England and Wales, and the Parties irrevocably submit to the exclusive jurisdiction of the Courts of England and Wales.

Schedule 1

Subject Matter of Processing

Provision of the APCS disclosure service

Duration of the Processing

Until such time as the Contract between the Controller and Processor for the provision of service ends.

Nature and Purpose of Processing

Provision for the APCS disclosure service to facilitate the submission of disclosure applications to the appropriate government disclosure bodies and the provision of the results received.

Where digital ID checks or digital right to work checks are ordered by the Controller, the processor will transfer the relevant personal data from the Controller to a UK Government registered Digital Identity & Attribute Service Provider, currently Yoti Ltd, who act as an independent Controller when processing those data for that purpose. The Processor's nature of processing for these digital ID checks is to pass the relevant personal data to the Digital Identity & Attribute Service Provider and to pass the resulting verification back to the Controller.

Where international background checks are ordered by the Controller, the Processor will transfer the relevant personal data from the Controller to the international checking organisation and provide any resulting reports back to the Controller. At present international background checks are performed by Owens Online LLC, a US based organisation, who act as an independent controller under UK GDPR and have enabled the UK Addendum to the EU Standard Contractual Clauses to enable the lawful transfer of personal data from the UK to the USA (including the processor to controller module for the export of the personal data required to perform the check).

Categories of Data Subjects

Current or prospective staff of the Controller (including employees, agency staff, volunteers) and applicable contractors.

Categories of Personal Data

Name, address, date of birth, place of birth, mother's maiden name, National Insurance Number, passport / driving licence details, contact details, results received from the disclosure service.

Special Categories of Personal Data and Criminal Offence Data

The personal data relating to the results received from the disclosure service constitute criminal offence data as described in Article 10 of UK GDPR and GDPR.

International Transfers

The Processor is a UK based entity and as such international transfers where the Controller is based in the EU or EEA are on the basis of the UK being an adequate nation for data protection purposes.

International Transfers relating to sub-processors are specified in the table below.

Transfers to Owens Online LLC in the USA are enabled via the UK Addendum to the EU Standard Contractual Clauses (specifically the processor to controller module).

Technical and Organisational Measures

The Processor agrees that they shall implement the following suitable measures to preserve the security of the data collected:

- All data are encrypted in transit and at rest (drive level encryption),
- The Processor shall ensure that their IT systems use modern software that is kept up-to-date,
- When personal data is deleted this will be done safely such that the data are irrecoverable,
- Appropriate back-up and disaster recovery solutions are in place,
- Where multi-factor authentication exists for the tools used to deliver the service the Processor shall have enabled it,
- The Processor maintains certification for Cyber Essentials Plus and ISO 27001
- Personal Data are anonymised according to the following default rules unless otherwise instructed by the Controller,

DBS application data

- 3 months after being started but not completed
- 3 months after being at the ID checking stage but not submitted
- 6 months after disclosure issue date
- For everything else, 24 months after the application was received by APCS

Credit check, overseas check, and education sector check data

- 6 months after the check was completed
- For everything else, 24 months after the check was ordered

Digital Id check data

- 24 months after the check was completed
- For errored or expired digital Id checks, 6 months after the check was ordered
- For everything else, 24 months after the check was ordered

Sub-Processors

List of Sub-Processors used by the Processor to deliver the agreed services which the Controller consents to

Name of Sub-Processor	Address (& details of transfer mechanism if not a UK organisation)	Nature of processing activity
Microsoft Ltd	Microsoft Campus, Thames Valley Park, Reading, Berkshire, UK, RG6 1WG	Office productivity tools
Vigo IT Solutions Ltd	The Lauries, 142 Claughton Road, Birkenhead, UK, CH41 6EY	Managed IT Services
Mailgun Technologies, Inc	112 E Pecan Street #1135 San Antonio, TX 78205, USA Certified with EU-US Data Privacy Framework, and the UK Extension to the EU-US Data Privacy Framework	Provision of email service for service messages
Simplified.ID Ltd	45 Market Street, Wirral, UK, CH47 2BQ	ID verification service and credit checks