KEYAPPS LTD – DATA PROCESSING AGREEMENT
(9th APRIL 2018)

This agreement comes into force from 25th May 2018 and shall replace any/all Terms and Conditions prior to that date.

Both parties hereby acknowledge and confirm that the Client is the "Data Controller" and KeyApps is the "Data Processor".

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, as described in Schedule 2;
"Services"	means those services and facilities described in Schedule 1 which are provided by the Data Processor to the Data Controller and which the Data Controller uses for the purpose(s) described in Schedule 1;
"Sub-Processor"	means a sub-processor appointed by the Data Processor to process the Personal Data; and
"Sub-Processing Agreement"	means an agreement between the Data Processor and a Sub-Processor governing the Personal Data processing carried out by the Sub-Processor, as described in Clause 10.

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

1.2.1 "writing", and any cognate 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 described in Schedule 2, 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 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 requiring the Data Processor to amend, transfer, delete, or otherwise dispose of the Personal Data.

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 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 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 (at the Data Controller's cost) 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 the European Economic Area (all EU member states, plus Iceland, Liechtenstein, and Norway) ("EEA") without the prior written consent of the Data Controller and, where the Data Controller consents to such a transfer to a country that is outside of the EEA, to comply with the obligations of Data Processors under the provisions applicable to transfers of Personal Data to third countries set out in Chapter 5 of the GDPR by providing an adequate level of protection to any Personal Data that is transferred;

4.8.2 not transfer any of the Personal Data 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 3, and take all steps necessary to protect the Personal Data against unauthorised or unlawful processing, accidental loss, destruction, damage, alteration, or disclosure. The Data Processor shall inform the Data Controller in advance of any changes to such measures;

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 in accordance with the requirements of Article 30(2) of the GDPR;

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 reasonable 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. The requirement to give notice will not apply if the Data Controller believes that the Data Processor is in breach of any of its obligations under this Agreement or under the law; and

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

5. Data Subject Access, Complaints, and Breaches

5.1 The Data Processor shall, at the Data Controller's cost, assist the Data Controller in complying with its obligations under the GDPR. In particular, the following shall apply to data subject access requests, complaints, and data breaches.

5.2 The Data Processor shall notify the Data Controller without undue delay if it receives:

5.2.1 a subject access request from a data subject; or

5.2.2 any other complaint or request relating to the processing of the Personal Data.

5.3 The Data Processor shall, at the Data Controller's cost, cooperate fully with the Data Controller and assist as required in relation to any subject access request, complaint, or other request, including by:

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

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

5.3.3 providing the Data Controller with any Personal Data it holds in relation to a data subject (within the timescales required by the Data Controller); and

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

5.4 The Data Processor shall notify the Data Controller immediately if it becomes aware of any form of Personal Data breach, 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 Article 37 of the GDPR, whose details are as follows: Paul Dawkins, paul.dawkins@keyapps.co.

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 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 or Sub-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 or Sub-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 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 term of the Service Agreement, 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 Controller 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. 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 15 days 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 shall not sub-contract any of its obligations or rights under this Agreement without the prior written consent of the Data Controller (such consent not to be unreasonably withheld).

10.2 In the event that the Data Processor appoints a Sub-Processor (with the written consent of the Data Controller), the Data Processor shall:

10.2.1 enter into a Sub-Processing Agreement with the Sub-Processor which shall impose upon the Sub-Processor the same obligations as are imposed upon the Data Processor by this Agreement and which shall permit both the Data Processor and the Data Controller to enforce those obligations; and

10.2.2 ensure that the Sub-Processor complies fully with its obligations under the Sub-Processing Agreement and the GDPR.

10.3 In the event that a Sub-Processor fails to meet its obligations under any Sub-Processing Agreement, the Data Processor shall remain fully liable to the Data Controller for failing to meet its obligations under this Agreement.

11. Deletion and/or Disposal of Personal Data

11.1 The Data Processor shall, at the written request of the Data Controller, delete (or otherwise dispose of) the Personal Data or return it to the Data Controller in the format(s) reasonably requested by the Data Controller within a reasonable time after the earlier of the following:

11.1.1 the end of the provision of the Services under the Service Agreement; or

11.1.2 the processing of that Personal Data by the Data Processor is no longer required for the performance of the Data Processor's obligations under this Agreement and the Service Agreement.

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):

a) The Data Processor will allow The Data Controller 15 days from termination of the Service Agreement to delete any/all data

b) After 15 days have elapsed, The Data Processor will remove from the active data sources and archive into an encrypted bundle, stored offline.

c) Should The Data Controller, and assuming there is no legal requirement for The Data Processor to keep such data, request that the archive be deleted, it will be.

12. Consideration

The Data Processor accepts the obligations in this Agreement in consideration of the payment of £1 from the Data Controller, which the Data Processor hereby acknowledges.

13. Law and Jurisdiction

13.1 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.

13.2 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

1) Mobile Application
2) Management System for the App
3) Website Plugin
4) Client's Website

The services perform the following function(s):

- Collection, collation, processing and transmission of applicant personal data, such as defined by The Data Controller, including profile, preferences and CVs and documents in line with the Service Level Agreement. Also, such information and personnel data supplied by The Data Controller in respect of their staff or organisational needs in the usage of the service.

- Facilitates data originating from The Data Controller's other systems to be stored, collated, and transmitted to the applicant.

SCHEDULE 2 contains a typical request in respect of data and is subject to agreement with The Data Contoller whereby it can be reduced or expanded.

SCHEDULE 2

Personal Data

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing
Name	Applicant Profile	Collection, Storage and Transmission to The Data Controller	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.
Home Address	Applicant Profile	Collection, Storage and Transmission to The Data Controller	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.
Telephone Number	Applicant Profile	Collection, Storage and Transmission to The Data Controller	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.
Email Address	Applicant Profile	Collection, Storage and Transmission to The Data Controller	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.
Occupation	Applicant Profile	Collection, Storage and Transmission to The Data Controller	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.
Filter Preferences	Applicant Profile	Collection, Storage and Transmission to The Data Controller	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.
CV	Documents	Collection, Storage and Transmission to The Data	To meet the requirements of the Service Level Agreement	Until such time The Data Contoller requests removal or

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing
		Controller	and requests made by The Data Controller	at Termination of the Agreement.
Timesheet	Documents	Collection, Storage and Transmission to The Data Controller	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.
Industry-Specific Documents (e.g. Certifications, Right to Work, Passport etc. as defined by The Data Controller)	Documents	Collection, Storage and Transmission to The Data Controller	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.
Client Information (as per detailed in SCHEDULE 1)	Client Data	Collection, Storage and Transmission to the Applicant or for such usage of the Service as defined by The Data Controller.	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.
Client Personnel Data (as per detailed in SCHEDULE 1)	Client Data	Collection, Storage and Transmission to the Applicant or for such usage of the Service as defined by The Data Controller.	To meet the requirements of the Service Level Agreement and requests made by The Data Controller	Until such time The Data Contoller requests removal or at Termination of the Agreement.

SCHEDULE 3

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 provided to the Data Controller on or before the commencement of this Agreement;

      2.1.4 is disseminated to all relevant staff; and

      2.1.5 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 form (for example, by using couriers rather than post) or electronic form (for example, by using RSA encryption);

   2.7 password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure (using a combination of upper and lower-case letters, special characters and numbers, and, where practicable, the passwords themselves will not be stored directly but will be subject to a computer hashing algorithm which will instead be stored), 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; and

2.9.3 notifying the Data Controller as soon as any such security breach occurs.

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 27001:2013, as appropriate to the Services provided to the Data Controller.