Data Protection Annex

1. DATA PROTECTION

1.1 For the purposes of this annex (**Data Protection Annex**), 'Data Protection Legislation' means the Data Protection Act 1998, and all applicable laws and regulations relating to the processing of personal data (including, where applicable, the guidance and codes of practice issued by any competent authority) and which shall include the national implementing law for the General Data Protection Regulation (2016/679/EU) which will replace the Data Protection Act 1998, when it enters into force (**Data Protection Legislation**).

1.2 AppRiver shall comply with all applicable Data Protection Legislation in relation to its obligations under this Data Protection Annex as a Data Processor. For the purposes of this Data Protection Annex, 'Personal Data' shall have the meaning ascribed to it in the Data Protection Legislation (**Personal Data**) and shall relate to Personal Data processed by AppRiver for or on behalf of Data Controller or any of its affiliates. **Data Controller** and **Data Processor** have the meanings as defined in the Data Protection Legislation.

1.3 The Exhibit to this Data Protection Annex sets out the scope, nature and purpose of processing of Personal Data by AppRiver under this Agreement (**Data Protection Purpose**), including details as to the duration of the processing, the types of Personal Data, which will be processed by AppRiver and categories of Data Subject (where **Data Subject** has the meaning as defined in the Data Protection Legislation). Any changes to the Data Protection Purpose must be agreed in writing between the Parties.

1.4 Data Controllers must ensure that they have all necessary appropriate consents and approvals in place to enable lawful transfer of the Personal Data to AppRiver for the duration and purposes of this Data Protection Annex.

1.5 Without prejudice to the generality of clause 1.2, AppRiver shall, in relation to any Personal Data processed in connection with the performance of its obligations under this Data Protection Annex:

(a) process that Personal Data only in accordance with the Data Protection Purpose and the written instructions of Data Controller from time to time in accordance with this Data Protection Annex, and for no other purpose unless the AppRiver is required by the laws of any member of the European Union or by the laws of the European Union applicable to AppRiver to process Personal Data (**Applicable Laws**). Where AppRiver is relying on laws of a member of the European Union or European Union law as the basis for processing Personal Data, AppRiver shall promptly notify Data Controller of this before performing the processing required by the Applicable Laws, unless those Applicable Laws prohibit AppRiver from notifying Data Controller;

(b) not disclose the Personal Data or information extracted from the Personal Data to third parties without the prior written approval of Data Controller and ensure that all

AppRiver personnel who have access to and/or process Personal Data are appropriately trained in compliance with the Data Protection Legislation and are aware of, and obliged to adhere to, the requirements to keep the Personal Data confidential;

(c) ensure that it has in place appropriate technical and organizational measures against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, as if it were the Data Controller in respect of that Personal Data, in compliance with the Data Protection Legislation, and shall provide Data Controller with any information which Data Controller reasonably requests in relation to the technical and organisational measures which it has implemented, and promptly comply with any requirements made by Data Controller to ensure that the technical and organisational measures comply with the Data Protection Legislation;

(d) not use a sub-processor unless expressly approved by Data Controller in writing. Where Data Controller does provide such consent, AppRiver will ensure that all sub-processors who have access to and/or process Personal Data are appropriately trained in compliance with the Data Protection Legislation and are aware of, and obliged to adhere to, the requirements to keep the Personal Data confidential. AppRiver must, as a pre-requisite to, and as an ongoing condition for, any sub-processing of Personal Data, have a written agreement in place with the third-party processor, providing no less protection than afforded to Data Controller under this Data Protection Annex;

(e) assist Data Controller, in responding to requests and/or complaints from any Data Subjects exercising their rights in relation to the Data Protection Legislation;

(f) assist Data Controller in complying with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(g) at the request of Data Controller, delete or return to Data Controller all Personal Data and copies thereof on termination of the relevant agreement between AppRiver and the Data Controller (or at any time as requested by Data Controller) unless and to the extent storage is required of the Data Processor by any Applicable Laws;

(h) make available to Data Controller, or any third party duly nominated by Data Controller, all information necessary to demonstrate AppRiver's compliance with the requirements of this Data Protection Annex and allow and reasonably assist with audits reasonably requested by Data Controller in relation to ascertaining AppRiver's compliance with this Data Protection Annex;

(i) not transfer any Personal Data outside of the European Economic Area without the prior written consent of Data Controller and where such consent is given by Data Controller, AppRiver will ensure that:

  (i) any transfer of Personal Data outside of the European Economic Area is in accordance with the written instructions and approval of Data Controller;

(ii) it has appropriate safeguards in relation to the transfer;

(iii) the Data Subject will still have enforceable rights and effective legal remedies;

(iv) it at all times, complies with its obligations under this Data Protection Annex, by providing an adequate level of protection to any Personal Data that is transferred; and

(v) it complies with any reasonable instructions notified to it in advance by Data Controller with respect to the processing and/or transferring of the Personal Data (for example, incorporating the latest EU-Standard Contractual Clauses (in relation to transfers of Personal Data outside of the EEA); and

(j) immediately inform Data Controller if any of Data Controller's instructions to AppRiver infringe the Data Protection Legislation.

1.6 Where AppRiver becomes aware of a data security breach, or any other relevant incident that affects the security or integrity of Personal Data (a **Personal Data Breach**), AppRiver shall:

(a) inform Data Controller promptly, and in any event within 24 hours of the relevant Personal Data Breach;

(b) provide to Data Controller all relevant information about the Personal Data Breach to assist any investigation by Data Controller and/or relevant regulator; and

(c) take any reasonable steps requested by Data Controller and/or relevant regulator in order to contain and respond to the Personal Data Breach.

Exhibit to Data Protection Annex

1. Description of the Processing Activities Data Subjects

Data Controller may submit personal data to AppRiver which may include but is not limited to, personal data related to the following categories:

- its clients or customers; and
- its staff.

2. Categories of data

The personal data transferred may include but is not limited to the categories of data set out below.

Personal Data

- Name
- Email Address
- Phone number
- Address
- Appraisal form
- National Insurance Number/Government ID numbers
- Financial details
- Communications monitoring (of email, internet usage etc)
- References
- Interview notes
- Leisure activities/interests
- Career history
- Cookie (online identifier)
- IP address (online identifier)
- Browser history details
- User activity details and user preferences
- Person's location
- Occupation
- Passport
- Biometric element (facial recognition)
- Description (from which a person is identifiable)

Sensitive Personal Data

- Race
- Ethnic origin
- Political opinion
- Religious beliefs
- Physical/mental health
- Sexual orientation
- Criminal offences (or proceedings which involve them).

3. Processing operations

The personal data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities:

- storage and other processing necessary to provide and maintain the Services provided to the Data Controller;
- to provide services and technical support to the Data Controller.