Data Processing Agreement

This Data Processing Agreement ("Agreement") forms part of the Contract for Services under FYI's Terms and Conditions ("Principal Agreement") between

[Name of company]

[Address of company]

[Address of company]

(the "**Company**")

and

FYI Software (UK) Ltd

85 Great Portland Street First Floor

London, W1W 7LT

(the "**Processor**")

(together as the "**Parties**")

WHEREAS

a) The Company acts as a Data Controller.

b) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Processor.

c) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing.

d) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

   1.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

   1.2. "Agreement" means this Data Processing Agreement and all Schedules;

   1.3. "Company Personal Data" means any Personal Data Processed by the Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

   1.4. "Data Protection Laws" means, to the extent applicable to the performance of the Services, the EU Data Protection Laws, UK Data Protection Laws and the applicable data protection or privacy laws of any other country;

   1.5. "EEA" means the European Economic Area;

1.6. “EU Data Protection Laws” means the GDPR, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time;

1.6.1. “GDPR” means EU General Data Protection Regulation 2016/679 and, as applicable, the UK GDPR;

1.6.2. “Services” means online secure services provided by the Data Processor pursuant to the Principal Agreement;

1.6.3. “Sub-processor” means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the provision of the Services;

1.6.4. “UK Data Protection Laws” means the GDPR as transposed into UK law pursuant to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) (“UK GDPR”), the Data Protection Act 2018, and any other laws applicable the processing of personal data and privacy, in each case as amended, replaced or superseded from time to time.

1.6.5. The terms, “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”,

1.6.6. “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in

1.6.7. the Data Protection Laws, and their cognate terms shall be construed accordingly.

2. Processing of company personal data

2.1. Processor shall:

2.2. comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.3. not Process Company Personal Data other than as set out in the Annex to this Agreement or otherwise on the relevant Company’s documented instructions.

2.4. The Company hereby instructs Processor to Process Company Personal Data in connection with the performance of the Services and warrants that it has all necessary notices, consents and approvals in place to provide the Company Personal Data to the Processor and its sub-processors for Processing in accordance with this Agreement.

3. Processor workers

3.1. Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with applicable laws in the context of that individual’s duties to the Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2. In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub-processing

5.1. Processor shall not appoint (or disclose any Company Personal Data to) any sub-processor unless required or authorized by the Company (acting reasonably). Any Sub-processor appointment shall be subject to a written agreement that contains clauses no less protective of the Company Personal Data as the terms of this Agreement, and the Processor shall remain liable for the acts and omissions of its sub-processors in connection with the Company Personal Data.

6. Data Subject Rights

6.1. Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2. Processor shall:

6.3. promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.4. ensure that it does not respond to that request except on the documented instructions of Company or as required by applicable laws to which the Processor is subject, in which case Processor shall to the extent permitted by applicable laws inform Company of that legal requirement before the Processor responds to the request.

7. Personal Data Breach

7.1. Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform the Supervisory Authority and/or Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2. Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

8.1. Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

9. Deletion or return of Company Personal Data

9.1. Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data, delete and procure the deletion of all copies of those Company Personal Data.

9.2. Processor may continue to store Company Personal Data to the extent required to comply with its legal obligations, including as required by Data Protection Laws or to the extent an exemption applies under Data Protection Laws.

10. Audit rights

10.1. Subject to this section 10, Processor shall make available to the Company on request all information reasonably necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Processor.

10.2. Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law. Any audit shall be subject to reasonable prior notice and agreement as to the date and time and conduct of the audit, and may be subject to supervision by the Processor.

11. Data Transfer

11.1. The Processor will not transfer the Data outside of the European Economic Area (EEA) nor the United Kingdom (UK) unless it has taken such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Law. Such measures may include (without limitation) transferring the Data to a recipient in a country that the European Commission and/or the UK Secretary of State (as applicable) has decided provides adequate protection for personal data (for example, New Zealand) or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission and/or UK Secretary of State or UK Information Commissioner (as applicable). To this end, Company authorises Processor to enter into standard contractual clauses with any recipient of Company Personal Data that is not located in a territory deemed adequate where this is necessary for the transfer of Company Personal Data for the proper performance of the Services.

12. General Terms

12.1. Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

12.2. disclosure is required by law;

12.3. the relevant information is already in the public domain.

12.4. Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1. Subject to clause 13.2, this DPA is governed by the same laws as the same jurisdiction which governs the Principal Agreement.

13.2. To the extent required to comply with the GDPR and UK GDPR, and only in relation to matters relating to the compliance of this DPA or a party's actions under it in relation to

GDPR or UK GDPR, this DPA shall also be governed by the laws of each Member State where EU Data Protection Laws and the UK Data Protection laws, as applicable.

13.3. Each party irrevocably submits to the jurisdiction described in clause 13.1 with respect to any disputes or claims arising under this DPA.

Annexure A – Data Processing Schedule

This Annex forms part of the Data Processing Agreement.

1. Subject matter and duration of processing of personal data

   The subject matter is the processing of personal data for the purpose of providing the Services and associated support.

   Data processing will continue for the duration of the Principal Agreement, plus the period stipulated in the data processing agreement in accordance with clause 9.1.

2. Nature and purpose of processing personal data
3. The nature of processing of personal data is to enable support as required for delivering the Services under the Principal Agreement.
4. Types of personal data processed

   The types of personal data processed may include:

   4.1. Names
   4.2. Contact details
   4.3. Tax identifiers like Unique Tax References and National Insurance numbers
   4.4. Age and dates of birth
   4.5. Financial, tax and payroll information
   4.6. Categories of data subjects

Note: FYI provides configurable Custom Fields which firms may use at their discretion. The nature and category of any data entered into Custom Fields, including any special category data, is determined and controlled by the firm, not by FYI

5. Categories of data subjects

   The categories of data subjects include:

   5.1. employees of the Company
   5.2. Clients of the company
   5.3. Directors, shareholders and employees of clients of the company
   5.4. Other professional contacts of the company
   5.5. Employees of service providers to the company”