DATA PROCESSING ADDENDUM

1. Definitions

1.1 In this Addendum the following terms have the following meanings:

"Addendum" means this Data Processing Addendum;

"Addendum Effective Date" means the earlier of:

(a) the date upon which we commence the provision of any services to you under the terms of the Agreement; or

(b) the date upon which you supply any of the Data to us.

"Applicable Data Protection Law" means as the context requires, either of:

(a) the Data Protection Act 2018 (**"UK DPA"**); or

(b) the General Data Protection Regulation ((EU) 2016/679) ("**EU GDPR**") and any laws made by an EU member state in pursuance of EU GDPR,

as may be amended, extended, re-enacted or replaced from time to time, along with the guidance and codes of practice issued by the UK's Information Commissioner or EU Commission (as applicable).

"Agreement" means the contract which is entered into between you and us, as further described in clause 2.2.1 of this Addendum.

"controller", "processor", "data subject", "personal data", "processing", "process" and **"special categories" of personal data**, whether capitalised or not, have the meanings given to such terms in Applicable Data Protection Law;

"**Customer", "you"** and **"yours"** etc has the same meaning as 'you' in the Agreement.

"**Data**" means the personal data as described in Annex B which is the subject of the processing undertaken by us on your behalf in pursuance of our obligations under the Agreement.

"**BigChange**", "**us**" "**our**" and "**we**" etc means the entity of BigChange Group's that is the party to the Agreement (i.e. the entity named in the services agreement as accepted).

"**BigChange's Group**" means, including BigChange, any and all members of the group of companies to which BigChange belongs, as may be amended from time to time.

"**BigChange Platform**" means the online platform, including but not limited to the underlying software and content which is owned by BigChange and/or its licensors, the use of which is licensed to you by BigChange subject to and in accordance with the terms of the Agreement.

"**Supervisory Authority**" means any independent public authority responsible for monitoring the application of the Applicable Data Protection Law in the relevant jurisdiction, including where UK DPA applies, the Information Commissioners Office.

2. Scope and application of this Addendum

2.1 This Addendum only applies if and to the extent:

2.1.1 you are a 'Controller' of the Data and we, as part of the services we are providing to you under the terms of Agreement, are processing the Data on your behalf as a 'Processor'; and

2.1.2 Either UK GDPR or EU GDPR apply to the Data that is being processed by us on your behalf.

2.2 Where it applies, this Addendum

2.2.1 is incorporated into and forms part of the Agreement.

2.2.2 supersedes and replaces any previous terms you and us may have entered into which concern the processing activities undertaken by us on your behalf in relation to the Agreement or any previous agreement ("**Previous DPA**") and, without prejudice to any accrued rights either you or we may have under any such Previous DPA, such Previous DPA will be terminated on and from the Addendum Effective Date.

3. Relationship of the parties and General Obligations

3.1 You hereby acknowledge and agree that, for the purposes of the Applicable Data Protection Law, you are the 'Controller' and you hereby appoint us as a 'Processor' of the Data.

3.2 Each of you and us agree to comply with all obligations that are imposed upon the parties respectively under Applicable Data Protection Law which relate to the processing of the Data hereunder.

3.3 Without affecting the generality of the obligation at clause 3.2, you acknowledge and agree that, as Controller, you shall retain control of the Data and undertake to:

3.3.1 provide to the relevant data subjects any required privacy notices and obtain from such individuals any required consents for the processing of the Data undertaken by us;

3.3.2 ensure that you have a lawful basis for any processing we are undertaking on your behalf; and

3.3.3 ensure that the instructions you provide to us for the processing of the Data are in compliance with Applicable Data Protection Laws.

4. Processing by BigChange

4.1 The details of the subject matter, duration of the processing, nature and purpose of the processing (the "**Permitted Purpose**") are as set out in Annex B of this Addendum.

4.2 We shall process the Data only

4.2.1 subject to clause 4.2.2, to the extent and in such manner as is necessary for the Permitted Purpose; and

4.2.2 in accordance with your documented instructions, including those set out in the terms of the Agreement (including this Addendum) and any other written instructions you provide to us to amend, transfer, delete or otherwise process the Data unless we become aware that such processing would or may result in a breach of Applicable Data Protection Laws in which case we shall:

4.2.2.1 notify you as soon as reasonably practicable upon us becoming aware: and

4.2.2.2 not be liable to you if, despite a notification made by us under clause 4.2.2.1, you insist on us processing the Data in accordance with your instructions.

5. International transfers

5.1 You agree that, subject to the provisions of clause 5.2, where necessary to enable us to perform our obligations under the Agreement (including to provide support), we may transfer the Data to other entities within BigChange's Group. You acknowledge and agree that this may result in the transfer of the Data to entities located in countries other than the UK or EU which are not subject to the same protection under local privacy laws. We may also transfer the Data in order for our third-party sub-processors so that they may provide the services for which they are engaged.

5.2 Where a transfer undertaken in pursuance of clause 5.1 is being made to a country that is not the subject of an adequacy decision/regulations, we undertake to have in place 'adequate safeguards' as required by Applicable Data Privacy Laws (for example, ensuring that the recipient has executed the EU standard contractual clauses and, where applicable UK addendum) to protect the Data that is the subject of the transfer.

6. Confidentiality of processing

We will ensure that any person we authorise to process the Data (an "**Authorised Person"**) will do so under a duty of confidence and at all times in accordance with our general confidentiality obligations under the Agreement. We shall ensure that Authorised Persons receive appropriate training on how to handle personal data and are aware of our obligations to protect the Data under Applicable Data Protection Laws.

7. Security

We will implement appropriate technical and organisational measures to protect the Data from any breach of security which results in: (i) accidental or unlawful destruction of; (ii) unauthorised disclosure of or access to; and/or (iii) loss of, damage to and/or alteration of, the Data (a "**Security Incident**"). The measures we will implement shall include those physical, technical and organisational measures, as set out in Annex A, provided that we reserve the right to amend and update these measures from time to time as we deem appropriate.

8. Subcontracting

8.1 Subject to the provisions of this clause 8, we will not engage another processor (a sub-processor) to process the Data.

8.2 You consent to the processing of the Data for the Permitted Purpose by:

8.2.1 any member of BigChange's Group including those members to which the data is transferred under clause 5.1; and

8.2.2 subject to the provisions of clause 8.3, any third-party sub-processor who is engaged to process the Data either us or such other member of BigChange's Group who processes the Data under clause 8.2.1.

8.3 We shall maintain or procure the maintenance of an up-to-date list of all third-party sub-processors which shall be available at https://www.bigchange.com and which you can check for updates. This list will be updated with details of any change in sub-processors at least 30 days prior to the change. You may object to the appointment or replacement of a third-party sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such an event, we will either,

8.3.1 not appoint or replace, or procure the non-appointment or replacement of, the sub-processor; or

8.3.2 where, notwithstanding your objection, the sub-processor is appointed or not replaced, ensure that such sub-processor is not involved in the processing of any of the Data, or

8.3.3 if we, in our sole discretion determine that neither of the measures at 8.3.1 or 8.3.2 are reasonably possible, allow you to suspend or terminate the Agreement without penalty, provided that you shall remain liable for any fees incurred by you up to and including the date of suspension or termination.

8.4 We undertake that:

8.4.1 any and all sub-processors shall be appointed subject to data protection terms that require such sub-processors to protect the Data to the standard required by Applicable Data Protection Law and on terms that are no less stringent than these; and;

8.4.2 we shall remain liable to you for any breach of this Addendum that is caused by an act, error or omission of any sub-processor.

9. Data subjects' rights

9.1 We will provide reasonable and timely assistance to you (including by taking appropriate technical and organisation measures) to enable you to comply with your obligations under Applicable Data Protection Law to respond to any requests made by data subjects to exercise their rights in relation to the processing of the Data undertaken by us. We shall:

9.1.1 promptly notify you if we or any of our sub-processors receive a request from a data subject; and

9.1.2 not respond to the request unless we receive your written instructions to do so or unless we are required to respond to the data subject under Applicable Data Protection Law.

10. General cooperation

10.1 We shall notify you if we receive any other correspondence, enquiry or complaint received from a data subject, Supervisory Authority or other third-party in connection with the processing of the Data under this Addendum and we shall provide you with all relevant details unless we are prohibited from doing so by Applicable Data Protection Law.

10.2 If we believe or become aware that the processing of the Data undertaken by us is likely to result in a high risk to the data protection rights and freedoms of data subjects, we will inform you and provide reasonable co-operation to you in connection with any data protection impact assessment and/or consultation with the Supervisory Authority that may be required under Applicable Data Protection Law.

11. Security incidents

If we become aware of a Security Incident, we will inform you without undue delay and will provide reasonable information and cooperation to you so that you can fulfil any data breach reporting obligations you may have under (and in accordance with the timescales required by) Applicable Data Protection Law. Following your written request, we will provide such reasonable assistance as you may require in order to investigate such Security Incident and we shall take reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident. We shall keep you informed of all material developments in connection with the Security Incident.

12. Costs

12.1 You shall reimburse us for our reasonable costs and expenses incurred in providing any assistance and co-operation required (including where we have taken any technical or organisational measure) under clauses 9, 10, or 11, unless the need for such assistance, co-operation or measures arises from any breach by us of this Addendum.

13. Deletion or return of data

13.1 Unless you provide written instructions to the contrary, you agree that we will retain the Data for as long as is necessary for the purpose for which it was collected. On expiry of this period, or if you request us to do so earlier, we will, at your election, either delete or return the Data and you agree that such deletion or return shall be made in such a manner and form determined by us, acting reasonably providing that it undertakes to do so securely. This requirement will not apply to:

13.1.1 the extent that we are required by Applicable Data Protection Law or other applicable law to retain some or all of the Data, in which case we will only process the data for the purpose and duration for which its retention is required by such law, or

13.1.2 to Data which is archived on back-up systems. In such cases, the data shall be securely isolated and retained in accordance with our back-up policies.

14. Evidence of compliance

14.1 Subject to clause 14.2, upon your reasonable request, we shall provide you with such information as is necessary to demonstrate our compliance with the terms of this Addendum.

14.2 Requests made under clause 14.1 shall not exceed more than one per contract year (the first contract year starting on the commencement date of the Agreement and each 12 month period thereafter during the term) unless you have reasonable grounds to expect that a Security Incident will occur or is occurring and such request is made in direct response to such Security Incident or suspected Security Incident.

15. Prohibited data

Unless explicitly requested by us to do so, you will not disclose (and will not permit any data subject to disclose) any special categories of personal data to us for processing. You agree that we shall have no liability whatsoever (including for any damage, loss, costs and expenses you may incur) as a result of your breach of this clause 15, irrespective of whether such liability arises in connection with a breach by us of the terms of this Addendum.

16. Governing Law

The provisions on governing law and jurisdiction as set out in the Agreement shall apply to this Addendum.

Annex A – Security measures

1. Technical Measures – BigChange product

1.1 Encryption
1.1.1 Data in transit is encrypted with TLS 1.2+
1.1.2 Data at rest is encrypted with either Serpent 256 or AES 256 encryption on disk

1.2 Access Authorisations, Passwords and Authentication
1.2.1 Access authorisations and password complexity rules are enforced
1.2.2 MFA/2FA is supported

1.3 Back-ups
1.3.1 Performed daily for all production systems, both application layer and customer data layer
1.3.2 Tested regularly
1.3.3 Stored offsite at a different data centre

1.4 Testing
1.4.1 Third-party penetration tests performed regularly
1.4.2 Automated software security scans performed weekly

2. Organisational Measures – BigChange

2.1 In-house IT Team
2.1.1 Monitors and maintains BigChange's internal systems

2.2 Training
2.2.1 BigChange staff undergo regular data security training

2.3 Access Authorisations, Passwords and Authentication
2.3.1 Access authorisations and password complexity rules are enforced
2.3.2 Access authorisations to customer data:
2.3.3 dual approval required
2.3.4 MFA/2FA enforced
2.3.5 password complexity and expiration enforced
2.3.6 private key authentication required
2.4 We are in the process of certifying for SOC2 Type 1.

3. Technical and Organisational Measures – Third-party Data Hosting Providers

We only use SOC2 and/or ISO27001 compliant third-party data hosting providers.

Annex B – Data processing schedule

1. Subject matter and duration of processing of personal data

The subject matter of personal data to be processed is that of the contacts of the Customer entered by or at the election of the Customer into the BigChange Platform. The duration of processing personal data shall be for as long as we have a business relationship with the Customer, and at the end of that relationship, we will act in accordance with clause 13 of this Addendum regarding deletion or return of such personal data.

2. Nature and purpose of processing personal data

The nature and purpose of processing personal data is in order to perform our obligations as set out in the Agreement in relation to providing the functionality of the BigChange Platform as set out in the Agreement and related documentation.

3. Types of personal data processed

The types of personal data processed include:

3.1 names
3.2 addresses
3.3 contact details
3.4 identification details (for example, tax registration numbers)
3.5 other personal data types which are required or related to use of the BigChange Platform

4. Categories of data subjects

The categories of data subjects include:

4.1 suppliers / service providers of Customer
4.2 customers / clients of Customer
4.3 employees / contractors of Customer
4.4 other contacts of the Customer