NOTE:

This e-bate Data Processing Addendum is intended for use only in relation to e-bate services where the parties have not entered into the separate e-bate Data Processing Agreement. The e-bate Data Processing Agreement can be accessed at the following website: www.e-bate.io.

Data Processing Addendum:

This Data Processing Addendum ("the Addendum") forms part of the pre-existing agreement ("the Commercial Agreement") between e-bate Limited of Unit 1, Brooks Park, Gaddesby Lane, LE7 4ZB ("e-bate") and the entity who has entered into the Commercial Agreement with e-bate Limited, together with any of its Affiliates who have a right to use the Applicable Services (as defined below) under the Commercial Agreement, (together the "Customer").

e-bate has agreed to supply software related services to the Customer under the terms of the Commercial Agreement, as more particularly detailed in the Commercial Agreement and the incorporated order form ("the Applicable Services"). In the course of providing the Applicable Services, it may be necessary for e-bate to receive and process certain Personal Data (as defined below) on behalf of the Customer.

This Addendum sets out the parties' obligations in relation to the processing of Personal Data which the Customer inputs into e-bates software and systems for the purpose of the Applicable Services.

The terms used in this Addendum have the meanings set out below. Capitalised terms not otherwise defined in this Addendum shall have the meanings given to them in the Commercial agreement. Except as modified below, the terms of the Commercial Agreement shall remain in full force and effect.

In consideration of the obligations set out below the parties agree that the terms and conditions set out below shall be added as an addendum to the Commercial Agreement. Except where the context requires otherwise, references in this Addendum to the Commercial Agreement are to the Commercial Agreement as amended by and including this Addendum.

1. DEFINITIONS

1.1 In this Addendum, the following definitions and rules of interpretation shall apply:

Affiliates	any entities that directly or indirectly control, are controlled by, or are under common control with the Customer and who have a right to use the Applicable Services.
Agreed Purpose	The purpose of providing the Applicable Services to the Customer in accordance with the terms of the Commercial Agreement.
Applicable Law	has the meaning given to it in clause 5.2 of this agreement.
Customer Personal Data	means all Personal Data inputted by the Customer into e-bate's software and/or systems or otherwise provided to e-bate by the Customer for the purposes

	of the Commercial Agreement and the provision by e-bate of the Applicable Services.
Data Protection Legislation	means all applicable laws, regulations, directives and codes of practice relating to the processing of personal data and privacy in the European Union and UK including, but not limited to the Data Protection Act 2018, the GDPR, the UK GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and the Electronic Communications Data Protection Directive (2002/58/EC) including any relevant primary, subordinate or implementing laws, regulations, directives, or codes of practice and any replacement/subsequent European and/or UK legislation, as amended from time to time.
EU Standard Contractual Clauses	the Standard Contractual Clauses annexed to the Commission Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries under the GDPR, as may be amended or replaced from time to time;
GDPR	means the General Data Protection Regulation (EU/2016/679).
Term	means the duration of the Commercial Agreement.
UK GDPR	means the UK retained EU law version of the General Data Protection Regulation ((EU) 2016/679).
UK Standard Contractual Clauses	means the UK versions of the Standard Contractual Clauses annexed to the Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data and the EU Standard Contractual Clauses as issued and amended by the UK Information Commissioner from time to time.

1.2 The terms **"Data Controller", "Data Processor"**, **"Data Subject"**, **"Personal Data"**, **"Process**" and **"Supervising Authorities"** shall be as defined by the Data Protection Legislation.

1.3 A reference to a statue or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

1.4 Any words following the terms including, include, in particular or for example or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

1.5 A reference to writing or written includes email.

2. AUTHORITY

2.1 The Customer warrants and represents that, before signing this Addendum it has been duly authorised to do so by any relevant Affiliates.

3. COMPLIANCE WITH DATA PROTECTION LEGISLATION

3.1 This Addendum sets out the framework for the sharing of Personal Data between the parties as Data Controller (Customer) and Data Processor (e-bate).

3.2 In the event that the Data Protection Legislation changes in a way that this Addendum is no longer adequate for the purpose of governing lawful data processing exercises, the parties will negotiate in good faith to amend this Addendum in light of such new legislation.

3.3 This Addendum is in addition to and does not relieve, remove or replace a party's obligations under the Data Protection Legislation. Both parties shall comply with all applicable requirements of the Data Protection Legislation.

4. NATURE, PURPOSE AND DURATION

4.1 The parties consider the sharing of Customer Personal Data is necessary for the provision of the Applicable Services under the Commercial Agreement. For the avoidance of any doubt the duration of processing of the Customer Personal Data shall be the same as the duration of the Commercial Agreement and, save as expressly provided for in the Commercial Agreement or this Addendum or as expressly agreed in writing to the contrary, all processing of Customer Personal Data by e-bate shall cease upon the termination of the Commercial Agreement.

4.2 It is noted and accepted by both parties that it is the Customer who is responsible for deciding what information is uploaded and provided to e-bate for the purpose of e-bate providing the Applicable Services.

4.3 e-bate shall not process any Customer Personal Data in a way that in incompatible with the Agreed Purpose.

4.4 Subject to the terms of the Commercial Agreement, the nature of the Processing to be carried out by e-bate may include the recording, organising, structuring, storing, adapting, retrieving, consulting, using, aligning or combining, restricting, erasing or destroying of Customer Personal Data in accordance with the terms of the Addendum.

5. CUSTOMER PERSONAL DATA TO BE PROCESSED

5.1 The categories of data subjects whose Personal Data may be processed by e-bate pursuant to this Addendum include the Customer's representatives and end users such as employees, job applicants, contractors, collaborators, partners, and customers as well as individuals who attempt to communicate or transfer Personal Data to users of the Applicable Services.

5.2 The types of Personal Data which may be processed by e-bate pursuant to this Addendum include personal contact information such as name, home address, home telephone or mobile number, fax number, email address and passwords as well as information concerning family, lifestyle, social circumstances such as age, date of birth, marital status, number of children and name(s) of spouse and/or

children; employment details such as employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualifications, identification numbers, social security details and business contact details. On occasion an individual's financial details may be processed as well as details of goods and services provided.

6. CUSTOMER OBLIGATIONS

The Customer shall:

6.1 ensure that it is entitled to transfer the Customer Personal Data to e-bate so that e-bate may lawfully use, Process and transfer such Personal Data in order to provide the Applicable Services for the duration and purpose of the Commercial Agreement;

6.2 be responsible for maintaining the accuracy of Customer Personal Data. For the Term of the Commercial Agreement, e-bate shall provide Customer access to the Customer Personal Data so that Customer may correct, delete, or block such Customer Personal Data. If the Customer is unable to correct, delete or block such Customer Personal Data, then to the extent permitted by law and pursuant to Customer's detailed written instructions, e-bate will make such corrections, amendments, or deletions on the Customer's behalf pursuant to a mutually agreeable statement of work in which Customer agrees to pay e-bate reasonable fees associated with the performance of any such correction, deletion or blocking of personal data; and

6.3 reimburse e-bate on a time and materials basis for all costs e-bate incurs in allowing audits or inspections pursuant to clause 7.1 below and providing assistance to the Customer pursuant to clauses 7.1, 7.6, 7.9, 7.10, 7.11 and 7.12 below, save that e-bate shall not be entitled to make any charge for providing any such assistance which is reasonably established by the parties to flow directly from any breach of the terms of this Addendum by e-bate.

7. E-BATE'S OBLIGATIONS

e-bate shall:

7.1 maintain and make available to the Customer sufficient records and information to demonstrate its compliance with the obligations laid down in the Data Protection Legislation and this Addendum, and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, provided that the Customer, or other such auditor mandated by the Customer, enter into an appropriate confidentiality agreement with e-bate prior to carrying out such audit or inspection and, save where such inspection or audit results from an actual or reasonably suspected personal data breach, giving e-bate at least 14 days written notice of its intention to carry out such an inspection or audit;

7.2 process the Customer Personal Data only in accordance with the documented instructions of the Customer during the Term including (but not limited to) those instructions documented in the Commercial Agreement, unless e-bate is required by the laws of England and Wales, by the national laws of any member of the European Union or by the laws of the European Union to process the Customer Personal Data (as appropriate) ("**Applicable Law**"). Where e-bate is relying on Applicable Law as the basis for Processing Customer Personal Data, it shall promptly

notify the Customer of the same before performing such Processing unless the Applicable Law prohibits e-bate from notifying the Customer;

7.3 promptly inform the Customer in the event that e-bate reasonably believes that the Customer's instructions breach the Data Protection Legislation;

7.4 treat the Customer Personal Data as strictly confidential;

7.5 ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful Processing of Customer Personal Data and against accidental loss or destruction of, or damage to Customer Personal Data. Having regard to the nature of the Customer Personal Data to be Processed, the state of technological development and the cost of implementing measures, the Customer acknowledges and agrees, that to the extent applicable to e-bates Processing of the Customer Personal Data, the measures set out at Annex A constitute appropriate technical and organisational measures to protect against the harm that might result from any such unauthorised or unlawful Processing or accidental loss, destruction or damage;

7.6 taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing, provide the Customer with full co-operation and assistance in ensuring compliance with the obligations laid down in the Data Protection Legislation concerning the security of its Processing including the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to that risk;

7.7 ensure that access to the Customer Personal Data is limited to those employees who need access to the Customer Personal Data to enable e-bate to fulfil its rights and obligations under this Addendum and under the Commercial Agreement and that such employees are obliged to keep the Customer Personal Data confidential. e-bate shall ensure that all of its employees with access to the Customer Personal Data:

(a) are informed of the confidential nature of the Customer Personal Data;
(b) have undertaken training in the laws relating to the handling of Personal Data; and
(c) are aware both of e-bate's duties and their personal duties and obligations under the Data Protection Legislation and this Addendum.

7.8 not transfer any Personal Data outside of the United Kingdom or European Economic Area other than as expressly permitted by clause 10 of this Addendum;

7.9 promptly inform the Customer of any complaints, requests or enquiries received from Data Subjects under the Data Protection Legislation, including but not limited to requests under Articles 15, 16, 17, 18, 20, 21 and/or 22 of the GDPR, and shall provide the Customer with full co-operation and assistance in relation to such complaints, requests or enquiries;

7.10 assist the Customer in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with Supervisory Authorities or regulators;

7.11 notify the Customer without undue delay, upon becoming aware of a personal data breach (the accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, or any other unlawful form of

processing) and co-operate fully with the Customer to the extent required with regard to the notification of the data breach to the relevant Supervisory Authority and the communication of the data breach to the affected Data Subject(s);

7.12 assist the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Customer reasonably considers to be required by articles 35 or 36 of the GDPR or UK GDPR.

7.13 not retain or process Customer Personal Data for longer than is necessary to carry out the Agreed Purpose and at the written direction of the Customer as detailed in the Commercial Agreement or if not detailed in the Commercial Agreement as subsequently directed in writing, delete or return Personal Data and copies thereof to the Customer on termination of the Commercial Agreement unless required by Applicable Law to store the Customer Personal Data;

8. SUBCONTRACTORS

8.1 The Customer and each Affiliate, hereby give e-bate a general authorisation to appoint subcontractors to carry out processing of Customer Personal Data pursuant to this Addendum in accordance with this clause 8 and any restrictions contained within the Commercial Agreement ("Subprocessors").

8.2 e-bate may continue to use those Subprocessors already engaged by it as at the date of this Addendum, subject to e-bate in each case as soon as practicable meeting the obligations set out in clause 8.4 below.

8.3 e-bate shall give the Customer prior written notice of the appointment of any new Subprocessor including full details of the processing to be undertaken by the Subprocessor. If within 30 days of receipt of that notice, the Customer notifies e-bate in writing of any objections to that proposed appointment e-bate shall not appoint any Subprocessor until reasonable steps have been taken to address the objections raised by the Customer.

8.4 With respect to each Subprocessor, e-bate shall:

(a) carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Commercial Agreement and this Addendum;
(b) ensure that the arrangement between e-bate and the Subprocessor is governed by a written contract including terms which offer at least the same level of protection for Customer Personal data as those set out in this Addendum and which meet the requirements of the UK GDPR and the GDPR;
(c) ensure that the Sub-processor is informed of the confidentiality of the Customer's Personal Data and is, and its employees (if any) are, contractually obliged to keep the Customer Personal Data confidential;
(d) in the event that Personal Data would be transferred to a third-country outside of the UK and/or European Economic Community ("EEC") as a result of the engagement of the Subprocessor by e-bate, ensure that the arrangement between e-bate and the Subprocessor provides a level of protection equivalent to the UK GDPR and/or GDPR and that the

agreement referred to at clause 8.4(b) above contains a transfer mechanism which is in accordance with clause 10.2 below; and

(e) Provide to the Customer upon request a copy of any such agreement with the Subprocessor with any commercially sensitive or otherwise confidential terms redacted.

9. ANONYMOUS DATA

9.1 e-bate may (i) compile anonymous statistical and other information related to the performance, operation and use of the Applicable Services, and (ii) use anonymized data from the Applicable Services environment in an aggregated form for security and operations management to create statistical analyses, and for research and development purposes (clauses (i) and (ii) are collectively referred to as 'Service Analyses'). e-bate may make Service Analyses publicly available. For the avoidance of any doubt, the Service Analyses will not incorporate any Customer Personal Data or confidential information and e-bate retains all intellectual property rights in the Service Analysis.

10. INTERNATIONAL DATA TRANSFERS

10.1 Where the Customer or any of its Affiliates are based outside the UK or European Economic Area ("EEA") and the provision of the Applicable Services will result in the transfer of Customer Personal Data outside the UK and/or EEA the Customer will ensure that such transfer is lawful and, where an adequacy decision and/or adequacy regulation (as appropriate), is not in place will ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the GDPR and/or UK GDPR. Where appropriate and reasonably requested by the Customer e-bate will enter into the EU Standard Contractual Clauses or UK Standard Contractual Clauses as requested by the Customer.

10.2 Other than as provided for by clause 10.1 above, where e-bate intends to transfer any Customer Personal Data outside of the UK and/or EEA for the purpose of providing the Applicable Services it shall ensure that such transfer is in compliance with the Data Protection Legislation and shall only permit the Processing of Customer Personal Data outside the UK and/ or EEA under the following conditions:

(a) e-bate and/or any third party it engages is processing Customer Personal Data in a territory which is subject to a current adequacy finding by the European Commission or a UK adequacy regulation exists confirming that the territory provides adequate protection for the privacy rights of individuals; or

(b) e-bate participates in a valid cross-border transfer mechanism under the Data Protection Legislation (including but not limited to use of the EU Standard Contractual Clauses and/or UK Standard Contractual Clauses (as appropriate)), so that e-bate (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of GDPR and UK GDPR; or

(c) the transfer otherwise complies with the Data Protection Legislation for the reasons notified by e-bate to the Customer in writing.

11. REVIEW AND TERMINATION THIS ADDENDUM

11.1 The parties shall continually review the effectiveness of this Addendum having consideration to Agreed Purpose. Where one party no longer feels that this Addendum is effective or appropriate the parties may agree to amend or terminate the Commercial Agreement.

11.2 The review of the effectiveness of this Addendum will involve:

(a) assessing whether the purposes for which the Customer Personal Data is being Processed are still the ones set out in this Addendum;

(b) assessing whether the Customer Personal Data is still as listed in this Addendum;

(c) assessing whether the Data Protection Legislation insofar as it governs data quality, retention, and Data Subjects' rights are being complied with; and

(d) assessing whether personal data breaches have been handled in accordance with this agreement and the Data Protection Legislation.

12. GENERAL PROVISIONS

12.1 The rights of the parties to terminate, rescind or agree any variation, waiver or settlement under the terms of the Commercial Agreement or this Addendum are not subject to the consent of any other person.

12.2 Variation. No variation of this Addendum shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

12.3 Severance. If any provision or part-provision of this Addendum is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this Addendum.

12.4 Each Party acknowledges that in entering into this agreement it does not rely on, and shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Addendum.

12.5 Each Party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misrepresentation based on any statement in this Addendum.

12.6 Rights and Remedies. The rights and remedies provided under this Addendum are in addition to, and not exclusive of, any rights or remedies provided by law or in the Commercial Agreement. For the avoidance of any doubt nothing in this Addendum shall modify the allocation of commercial risks agreed upon by the parties in the Commercial Agreement, including (but not limited to) any limitations or exclusions of liability.

12.7 Governing Law. This Addendum and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

12.8 Jurisdiction. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-

contractual disputes or claims) arising out of or in connection with this Addendum or its subject matter or formation

This Addendum has been entered into on the date on which the Commercial Agreement is executed.

SIGNED for and on behalf of

e-bate Limited

Name

Position

Signature

SIGNED for and on behalf of

The Customer

Customer Name

Name

Position

Signature

Exhibit A to the e-bate Data Processing Addendum

Access Control to Processing Areas (Physical Controls)

Data importer implements the following measures to prevent unauthorised persons from gaining access to the data processing equipment where the personal data is processed or used:

- Establishing security areas;
- Procuring 24-hour security service at data centres;
- Requiring all doors to be locked before and after entry;
- Restricting and protecting access paths;
- Securing the data processing equipment;
- Establishing access authorisations for staff and third parties, including the respective documentation;
- Restricting issuance of card-keys;
- Regulating card-keys once issued;
- Logging, monitoring and tracking all access to the data centre; and
- Securing the data centre with a security alarm system, and other appropriate security measures.

Access and Input Control of Data Processing Systems, Including Specific Areas of the Data Processing Systems (Technological Controls)

Data importer implements the following measures to prevent unauthorised persons from gaining access to the data processing systems, including specific areas of the data processing systems. Input and removal of personal data is also controlled by:

- Issuing and securing staff identification codes;
- Authenticating authorised personnel use at the individual level requiring authentication credentials such as user IDs that cannot be re-assigned to another person;
- Assigning individual terminals and/or terminal users and/or terminal users and host identification characteristics exclusive of specific functions;
- Limiting staff access to only that personal data relevant to the scope of each individual's role or responsibility. Personal data cannot be read, copied or modified or removed without authorisation;
- Electronic recording of input entries;
- Identifying and tracking terminal use at the user level;
- Regularly re-using and destroying tape back-up copies in a manner that renders the personal data un-readable; and
- Using industry standard encryption technologies. **Please note; data at rest will not be encrypted.**

Segregation of Personal Data (Technological Controls)

Data importer implements the following measures to process personal data gathered for unrelated purposes separately;

- Segregating personal data through the use of application security measures and then assigning access to the appropriate users;
- Separating personal data into modules within the data processing system. Each module is created for the specific purpose for which the personal data was gathered, i.e. by functionality and function; and
- Storing personal data in different areas at the database level on a per module or function basis.

Transmission Control (Technological Controls)

Data importer implements the following measures to prevent unauthorised persons from reading, copying, altering or deleting personal data during personal data transmission;

- Using firewall and encryption technologies to protect the gateways and pipelines through which personal data travels; and
- logging, monitoring and tracking transmissions in a manner that is commercially reasonable.

Availability Control (Process Controls)

Data importer implements the following measures to ensure that personal data is protected from accidental destruction or loss:

- implementing infrastructure redundancies to ensure data access is restored within seven days and backup performed at least weekly;
- storing back-ups off-site and ensuring they are readily available for restoration in case of failure of storage infrastructure for relational database server; and
- recording any detected security incident and deploying data recovery procedures as needed, including, if possible, identification of the person who carried them out.

Roles, Responsibilities and Policy Controls

Data importer implements the following measures to ensure personal data is processed only in accordance with instructions provided by data exporter:

- binding policies and procedures for data importer's employees and sub-processors. Policies will clearly inform staff of their obligations (including confidentiality and associated statutory obligations) and the associated consequences of any violation;
- individual appointment of system administrators;
- maintaining a current list with system administrators; identification details (e.g. name, surname, function or organisational areas);
- correcting any inaccuracies, and deleting personal data as instructed;
- implementing compliance audits;
- maintaining applicable third-party certifications that include audit reporting that can be produced upon request of data exporter; and
- establishing processes for the destruction or return of personal data to data exporter at the expiration or termination Customer's services agreement.