DATA PROCESSING ADDENDUM

This Data Processing Addendum (the **"Addendum"**) forms part of the Terms of Service entered into by and between Matt Bearman Ltd, trading as Saber, having its place of business at 269 Farnborough Road, Farnborough, Hampshire, GU14 7LY, England (**"Provider"**) and **_____** (**"Client"**) dated **_____** pursuant to which Provider provides services, including the use of the Provider's Saber Feedback Application and any other services purchased by Client from Provider (**"Services"**) to Client (the **"Agreement"**).

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not defined herein shall have the meaning set forth in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum. Each reference to the Addendum in this Addendum means this Addendum including its Schedules and Appendices.

In the course of providing the Services to Client pursuant to the Agreement, Provider may Process Personal Data on behalf of Client and the parties agree to comply with the following provisions with respect to any Personal Data.

1. Effectiveness

1.1 **Legal Authority.** Client signatory represents to Provider that he or she has the legal authority to bind Client and is lawfully able to enter into contracts (e.g., is not a minor).

1.2 **Termination.** This Addendum will terminate upon the earliest of: (i) termination of the Agreement as permitted hereunder or by the Provider's Terms and Conditions (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination); (ii) as earlier terminated pursuant to the terms of this Addendum or (iii) as agreed by the parties in writing.

2. Definitions

"Client Personal Data" means any Personal Data Processed by Matt Bearman Ltd (or a Sub- processor) on behalf of Client pursuant to or in connection with the Agreement;

“Data Protection Laws” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, and the GDPR, applicable to the Processing of Client Personal Data under the Agreement which are applicable to Client.

“GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

“Sub-processor” means any person (including any third party, but excluding an employee of Provider or any of its sub-contractors) appointed by or on behalf of Processor to Process Personal Data on behalf of Client under the Agreement

The terms, **"Commission"**, **"Controller"**, **"Data Subject"**, **"Member State"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing"**, **“Processor”**, and **"Supervisory Authority"** shall have the same meaning as in the GDPR, and shall be construed accordingly.

3. Processing of Personal Data

3.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Data Controller, Provider is a Data Processor and that Provider will engage Sub-processors pursuant to the requirements set forth in Section 5 **“Sub-processors”** below.

3.2 **Client Authority.** Client represents and warrants that it is and will at all relevant times remain duly and effectively authorized to give the instruction set forth in Section 3.4 below on behalf of itself.

3.3 **Client’s Processing of Personal Data.** Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. Client’s instructions for the Processing of Personal Data shall comply with Data Protection Laws. In addition, Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.

3.4 **Provider’s Processing of Personal Data.**

1. Provider shall only Process Client Personal Data for the purpose of the provision of the Services under the Agreement and in accordance with Client’s documented instructions which are consistent with the terms of the

Agreement, unless Processing is required by Data Protection Laws to which Provider (or the applicable sub-processor) is subject, in which case Provider shall to the extent permitted by the Data Protection Laws inform Client of that legal requirement before the relevant Processing of that Client Personal Data.

2. This Addendum, the Agreement and any Order Forms thereunder, are Client's complete and final instructions to Provider for the Processing of Client Personal Data. Any additional or alternate instructions must be agreed upon separately.

3. The following are deemed instructions of the Client to Provider: The processing of Client Personal Data (i) in accordance with the Agreement, this Addendum and any Order Forms under the Agreement, including without limitation with the transfer of Client Personal Data to any country or territory; and (ii) to comply with other documented instructions provided by Client where such instructions are consistent with the terms of the Agreement.

3.5 **Details of the Processing.** The subject-matter of Processing of Client Personal Data by Provider is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Client Personal Data and categories of Data Subjects Processed under this Addendum, as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws, are further specified in Exhibit A to this Addendum, as may be amended by the parties from time to time .

4. Provider Personnel

Throughout the term of this Addendum, Provider shall restrict its personnel from Processing Client Personal Data without authorization by Provider and shall limit the Processing to that which is needed for the specific individual's job duties in connection with Provider's provision of the Services under the Agreement. Provider will impose appropriate contractual obligations on its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. Sub-processors

5.1 **Appointment of Sub-processors.** For the purpose of the appointment of Sub-processors, Client acknowledges and agrees that Provider may engage third-party Sub- processors in connection with the provision of the Services, including without limitation the Processing of Client Personal Data.

5.2 **List of Current Sub-processors and Notification of New Sub- processors.** When requested by the Client, the Provider shall make available to Client an up-to-date list of all Sub- processors used for the processing of Client Personal Data.

5.3 **Objection Right for New Sub-processors.** Provider shall give Client prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. If, within 14 days of receipt of that notice, Client notifies Provider in writing of any objections (on reasonable grounds) to the proposed appointment, then (i) Provider shall work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and (ii) where such a change cannot be made within 14 days from Provider's receipt of Client's notice, notwithstanding anything in the Agreement, Client may by written notice to Provider with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.

5.4 **Sub-processing Agreement; Liability.** Provider has or shall enter into a written agreement with each Sub-processor (the **“Sub-processing Agreement”**) containing data protection obligations not less protective than those in the Agreement and/or this Addendum with respect to the protection of Client Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Provider shall be liable for the acts and omissions of its Sub-processors to the same extent Provider would be liable if performing the services of each Sub-processor directly under the terms of this Addendum.

5.5 **Copies of Sub-Processor Agreements.** Provider shall provide to Client for review copies of the Sub-processor agreements as Client may reasonably request from time to time. The parties agree that all commercial information may be removed by the Provider beforehand.

6. Security

6.1 **Adequate Measures.** 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, Provider shall in relation to the Client Personal Data implement and maintain throughout the term of this Addendum, the technical and organizational measures set forth in Exhibit B (the **"Security Measures"**). Client acknowledges and agrees that it has reviewed and assessed the Security Measures and deems the appropriate for the protection of Client Personal Data.

6.2 **Personal Data Breach Risk.** In assessing the appropriate level of security, Provider shall take account of the risks that are presented by Processing, in particular from a Client Personal Data Breach

7. Data Subject Rights

7.1 **Correction, Blocking and Deletion.** Provider shall comply with any commercially reasonable request by Client to correct, amend, block or delete Client Personal Data, as required by Data Protection Laws, to the extent Provider is legally permitted to do so.

7.2 **Measures to assist with Data Subject Rights.** Taking into account the nature of the Processing, Provider shall assist Client by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Client's obligations, as reasonably understood by Client, to respond to requests to exercisee Data Subject rights under the Data Protection Laws. To the extent legally permitted, Client shall be responsible for any costs arising from Provider's provision of such assistance.

7.3 **Response to Requests:** Provider:

1. shall promptly notify Client if it or any Sub-processor receives a request from a Data Subject under any Data Protection Laws & Regulation in respect of Client Personal Data; and

2. shall not and shall ensure that no Sub-processor responds to that request except on the documented instructions of Client or as required by Data Protections Laws to which Provider or Sub- processor is subject, in which case Provider shall, to the extent permitted by such Data Protections Laws inform Client of that legal requirement before it or the applicable Sub-processor responds to the request.

8. Personal Data Breach

8.1 **Notification of Data Breach.** Provider shall, to the extent permitted by law, notify Client without undue delay upon Provider or any Sub-processor becoming aware of a Personal Data Breach affecting Client Personal Data, providing Client with sufficient information to allow Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 **Assistance to Client** Provider shall co-operate with Client and take such reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Provider shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client reasonably considers to be required of it by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law & Regulation, in each case solely in relation to Processing of Client Personal Data by, and taking into account the nature of the Processing and information available to, Provider or the Sub-processors

10. Return or Destruction of Personal Data.

10.1 **Return or Deletion.** Subject to the provisions of Section 10.2 below, at Client's election, made by written notice to Provider following 30 days of the date of cessation of any Services involving the Processing of Client Personal Data (the **"Cessation Date"**), Provider shall, and shall procure that all Sub-processors: (a) return a complete copy of all Client Personal Data to Client in such format and manner requested by Client and reasonably acceptable to Provider; and (b) delete and procure the deletion of all other copies of Client Personal Data Processed by Provider or any Sub-processor. Provider shall comply with any such written request within 30 days of the Cessation Date.

10.2 **Retention of Copies.** Provider and each Sub-processor may retain Client Personal Data to the extent required by applicable European Union law or the law of an EU Member State and only to the extent and for such period as required by such laws and always provided that Provider shall ensure the confidentiality of all such Client Personal Data and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in such law requiring its storage and for no other purpose.

11. Audit.

11.1 **Report on Compliance.** Subject to the provisions of Section 11.3 below, at Client's written request, Provider will provide Client all information necessary to demonstrate compliance with this Addendum. To the extent Provider has acquired a confidential Service Organization Control (SOC) 2 Report (or a comparable report) on its systems examining logical security controls, physical security controls, and system availability, as produced by a third party auditor in relation to the Services

(**"SOC 2 Report"**), Provider will provide such report. The information provided will constitute Provider Confidential Information under the confidentiality provisions of the Agreement or a non-disclosure agreement, as applicable.

11.2 **Audit.** Provider shall allow for and contribute to audits, including inspections, by any Client or an auditor mandated by Client in relation to the Processing of the Client Personal Data by Provider or Sub-processors in accordance with Sections 11.1 and 11.3 to this Addendum.

11.3 **Process.** The parties agree that the audits described in Section 11.2 above and/or in the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

1. Client may contact Provider in accordance with the **"Notices"** Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Client may also review the SOC 2 Report or another audit of Provider's systems by and independent third party (**"Third Party Audit"**) if such a report is available.

2. Client shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Provider or Sub-processor premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

3. Before the commencement of any such on-site audit, Client and Provider shall mutually agree upon the scope, timing, and duration of the audit.

4. Provider or Sub-processor need not give access to its premises for the purposes of such an audit or inspection:
    a. to any individual unless he or she produces reasonable evidence of identity and authority;

    b. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Client undertaking an audit has given notice to Provider that this is the case before attendance outside those hours begins; or

    c. for the purposes of more than one audit or inspection, in respect of Provider or each Sub-processor, in any calendar year, except for any additional audits or inspections which: (A) Client reasonably considers necessary because of genuine concerns as to Provider's or applicable

Sub- processor's compliance with this Addendum; or (B) Client is required or requested to carry out by Data Protection Law and Regulation, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory; where Client has identified its concerns or the relevant requirement or request in its notice to Provider.

11.4 **Following the Audit:**

1. If Client chooses to conduct an independent audit rather than rely on a current SOC 2 Report or current Third Party Audit, if applicable and available, or if Client makes such choice because a current SOC 2 Report or current Third Party Audit is not available, Client will be responsible for any fees charged by any auditor appointed by Client to execute any such audit. Provider will provide Client with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit.

2. Client shall promptly notify Provider with information regarding any non-compliance discovered during the course of an audit.

12. Jurisdiction and Governing Law.

12.1 **Law.** This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the United Kingdom.

12.2 **Jurisdiction.** With respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity the parties submit to the jurisdiction of the competent courts of London, United Kingdom.

13. Indemnification; Limitation of Liability

If one party is held liable for a violation of this Addendum or, if applicable, any provision of the Standard Contractual Clauses, committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred in accordance with the provisions of the "Indemnification" Section of the Agreement. Each party's liability, taken together in the aggregate, arising out of or related to this Addendum and/or the Standard Contractual Clauses, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement. For the

avoidance of doubt, Provider's total liability for all claims from the Client or any third party arising out of or related to the Agreement and this Addendum shall apply in the aggregate for all claims under both the Agreement and this Addendum. Any indemnification

[Remainder of Page Intentionally Left Blank; Signature Pages to Follow]

EXECUTED by and on behalf of:
Provider

…….

Name: ……...

Role: …….

Date: …….

EXECUTED by and on behalf of:
Client

…….

Name: ……...

Role: …….

Date: …….

EXHIBIT A TO DATA PROCESSING ADDENDUM: DETAILS OF PROCESSING

Duration of the Processing: The duration of data processing shall be for the term agreed between data exporter and Provider in the Agreement or an applicable Order Form.

Nature and purpose of the Processing: The scope and purpose of processing of the data subjects' personal data is to facilitate the provision of Provider's Services.

Types of Client Personal Data: The personal data transferred includes e-mail, documents and other data in an electronic form provided in the context of Provider's Services.

Categories of Data Subjects: Data subjects include the Client's representatives and end- users including employees, contractors, collaborators, and Client's customers. Data subjects may also include individuals attempting to communicate or transfer personal information to users of Provider's Services. The data subjects exclusively determine the content of data submitted to Provider.

EXHIBIT B TO DATA PROCESSING ADDENDUM: SECURITY MEASURES

1. Personnel. Data Importer’s personnel will not process customer data without authorization. Personnel are obligated to maintain the confidentiality of any customer data and this obligation continues even after their engagement ends.

2. Data Privacy Contact

Matt Bearman Ltd.
Attn: Matt Bearman
269 Farnborough Road, Farnborough, Hampshire, GU14 7LY

3. Technical and Organization Measures. The Data Importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

3.1 Organization of Information Security.

a. *Security Roles and Responsibilities.* The Data Importer has appointed Matt Bearman as the security officer responsible for coordinating and monitoring the security rules and procedures.

b. *Duty of Confidentiality.* The Data Importer's personnel with access to customer data are subject to confidentiality obligations.

3.2 Risk Management.

The Data Importer conducts regular testing and monitoring of the effectiveness of its safeguards, controls, systems, including conducting penetration testing. The Data Importer implements measures, as needed, to address vulnerabilities discovered in a timely manner.

3.3 Storage.

The Data Importer's database servers are hosted in a data center operated by a third party vendor, that has been qualified per the Data Importer's vendor management procedure. The Data Importer maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to customer data.

3.4 Asset Management.

1. *Asset Inventory.* The Data Importer maintains an inventory of all media on which customer data is stored. Access to the inventories of such media is restricted to authorized personnel.

2. *Asset Handling.*

    a. The Data Importer employees are required to utilize encryption to store data in a secure manner and are required to use two-factor authentication to access Matt Bearman Ltd. networks.

    b. The Data Importer imposes restrictions on printing customer data and has procedures for disposing of printed materials that contain customer data.

    c. The Data Importer's personnel must obtain authorization prior to storing customer data on portable devices, remotely accessing customer data, or processing customer data outside the Data Importer's facilities.

3.5 Software Development and Acquisition: For the software developed by Data Importer, Data Importer follows secure coding standards and procedures set out in its standard operating procedures.

3.6 Change Management: Data Importer implements documented change management procedures that provide a consistent approach for controlling, implementing, and documenting changes (including emergency changes) for the Data Importer's software, information systems or network architecture. These change management procedures include appropriate segregation of duties.

3.7 Third Party Provider Management: In selecting third party providers who may gain access to, store, transmit or use customer data, Data Importer conducts a quality and security assessment pursuant to the provisions of its standard operating procedures.

3.8 Human Resources Security. The Data Importer informs its personnel about relevant security procedures and their respective roles, as well as of possible consequences of breaching the security rules and procedures. Such consequences include disciplinary and/or legal action.

3.9 Physical and Environmental Security.

1. *Physical Access to Facilities.* The Data Importer limits access to facilities where information systems that process customer data are located to identified authorized individuals who require such access for the performance of their job function. Data Importer terminates the physical access of individuals promptly following the date of the termination of their employment or services or their transfer to a role no longer requiring access to customer data.

2. *Physical Access to Components.* The Data Importer maintains records of the incoming and outgoing media containing customer data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of customer data they contain.

3. *Protection from Disruptions.* The Data Importer uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or line interference.

4. *Component Disposal.* The Data Importer uses commercially reasonable processes to delete customer data when it is no longer needed.

3.10 Communications and Operations Management.

1. *Security Documents.* The Data Importer maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel.

2. *Data Recovery Procedures.*

    a. On an ongoing basis, the Data Importer maintains multiple copies of customer data from which it can be recovered.

    b. The Data Importer stores copies of customer data and a data recovery procedures in a different place from where the primary computer equipment processing the customer data is located.

    c. The Data Importer has procedures in place governing access to copies of customer data.

    d. The Data Importer has anti-malware controls to help avoid malicious software gaining unauthorized access to customer data.

3. *Encryption; Mobile Media.* The Data Importer uses HTTPS encryption on all data connections. The Data Importer restricts access to customer data in media leaving its facilities. The Data Importer further has a destruction policy for hardware in the data center that stores customer data.

4. *Event Logging.* The Data Importer logs the use of our data-processing systems. We maintain logs for at least 10 days.

3.11 Access Control.

1. *Records of Access Rights.* The Data Importer maintains a record of security privileges of individuals having access to customer data.

2. *Access Authorization.*

    a. The Data Importer maintains and updates a record of personnel authorized to access systems that contain customer data.

    b. The Data Importer deactivates authentication credentials of employees or contract workers immediately upon the termination of their employment or services as well as such authentication credentials that have not been used for a period of time not to exceed six months.

c. The Data Importer identifies those personnel who may grant, alter or cancel authorized access to data and resources.

3. *Least Privilege.*

    a. Technical support personnel are only permitted to have access to customer data when needed for the performance of their job function.

    b. The Data Importer restricts access to customer data to only those individuals who require such access to perform their job function.

4. *Integrity and Confidentiality.*

    a. The Data Importer instructs its personnel to disable administrative sessions when leaving the Data Importer's premises or when computers are unattended.

    b. The Data Importer stores passwords in a way that makes them unintelligible while they are in force.

5. *Authentication.*

    a. The Data Importer uses commercially reasonable practices to identify and authenticate users who attempt to access information systems.

    b. Where authentication mechanisms are based on passwords, the Data Importer requires the password to be at least eight characters long.

    c. The Data Importer ensures that de-activated or expired identifiers are not granted to other individuals.

    d. The Data Importer maintains commercially reasonable procedures to deactivate passwords that have been corrupted or inadvertently disclosed or pursuant to a number of failed login attempts.

    e. The Data Importer uses commercially reasonable password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

6. *Network Design.* The Data Importer has controls to avoid individuals assuming access rights they have not been assigned to gain access to customer data they are not authorized to access.

3.12 Network Security.

1. *Network Security Controls.* Data Importer's information systems have security controls designed to detect and mitigate attacks by using logs and alerting.

2. *Antivirus.* Data Importer implements endpoint protection on its hosting environments, including antivirus; which are continuously updated with critical patches or security releases in accordance with Data Importer's server change control procedures.

3.13 Information Security Incident Management.

1. *Record of Breaches.* The Data Importer maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

2. *Record of Disclosure.* The Data Importer tracks disclosures of customer data, including what data has been disclosed, to whom, and at what time.

3.14 Business Continuity Management. The Data Importer employs redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original state from before the time it was lost or destroyed.