DATA PROCESSING AGREEMENT

Terms and Conditions relating to the processing of Personal Data

1. Definitions

1.1 Defined terms not otherwise specified in this DPA shall have the meaning attributed to them in the Terms and Conditions of Sale.

1.2 **Applicable Law:** means any law, statute, bye-law, regulation, order, regulatory policy, guidance or industry code, rule of court or directives or requirements of any regulatory body, delegated or subordinate legislation or notice of any regulatory body in the UK, EU or Member State Law to which Company or the Supplier is subject.

1.3 **Data Protection Laws:** means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation: (a) United Kingdom General Data Protection Regulation, Retained Regulation (EU) 2016/679 ("**UK GDPR**"); (b) the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); (c) any applicable national laws and regulations that implement the UK GDPR; and (d) the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) (as may be amended by the proposed Regulation on Privacy and Electronic Communications) ("**e-Privacy Laws**").

1.4 **Controller or Data Controller, Processor or Data Processor, Data Protection Officer, Data Subject, Personal Data Breach, Processing, Data Protection Impact Assessment** and **Supervisory Authority** shall have the same meaning attributed to them under Data Protection Laws, and **Process** and **Processed**, in the context of Processing Personal Data, shall be construed accordingly.

1.5 **Group**: shall mean the Supplier, any subsidiary company or any holding company from time to time of the Supplier, and any subsidiary from time to time of a holding company of the Supplier.

1.6 **Personal Data**: shall have the same meaning attributed to it under Data Protection Laws, but limited to data that is provided by the Company to the Supplier as part of the Services provided by the Supplier under the Agreement.

1.7 **Regulator**: shall mean any Supervisory Authority, Information Commissioner's Office or other regulator authorised under Applicable Law.

2. Application and Priority

2.1 The provisions set out in this Schedule are supplemental to the existing provisions set out in the Agreement. In the event of any conflict between the provisions of the Agreement and this Schedule, the provisions in this Schedule shall prevail and shall constitute a valid variation of the conflicting provisions in accordance with the terms of that Agreement. This Schedule shall be interpreted by the Parties in a manner that is compliant and consistent with Data Protection Laws. Nothing in this Schedule shall act to prevent either Party from complying with their respective obligations under Data Protection Laws.

3. Relationship of the Parties

3.1 The Parties agree that the Supplier Processes various types of Personal Data on behalf of the Company in relation to the performance and receipt of the Services.

3.2 Each Party shall comply with its obligations under this Schedule and under Data Protection Laws with respect to the types of Personal Data it processes and according to its responsibilities as a controller, joint-controller, processor or sub-processor (as appropriate) for the relevant Personal Data, as described in this Schedule.

3.3 Where the Company is acting as a Processor with respect to Personal Data and the Supplier is acting as a Sub-Processor with respect to that Personal Data, then:

a. the Processor shall be required to take steps to ensure that the Controller complies with its obligations under Data Protection Laws, including those referred to in clause 4.1; and

b. the Sub-Processor shall be deemed to be a Processor for the purposes of interpreting clause 5.

4. Controller Obligations

4.1 Whenever the Company is acting in a capacity as a Controller in relation to Personal Data, it shall comply in all respects with Data Protection Laws including:

a. by Processing such Personal Data fairly and lawfully, including by providing appropriate privacy notices to those Data Subjects in relation to whom that Party is Processing Personal Data as a Controller;

b. by implementing appropriate technical and organisational measures to protect such Personal Data as required under Data Protection Laws;

c. by ensuring that it has obtained consent to the standards required by Data Protection Law if such consent is required to contact any particular Data Subject under e-Privacy Laws; and

d. by determining if further details of the Processing to be undertaken by a Processor pursuant to this Schedule need to be recorded in the relevant Data Processing Details Form to comply with Data Protection Laws.

5. Processor Obligations

Where a Party is acting as a Processor of Personal Data on behalf of the other Party under this Agreement, the following provisions shall apply:

5.1 **General Processor Obligations**

a. The Supplier shall Process the Personal Data as necessary: (i) to perform its obligations under the Agreement; (ii) to comply with its obligations under Applicable Laws; and (iii) for such other purposes as may be described in the Data Processing Details Form (the "Permitted Purpose"), except where otherwise required by any Applicable Law. In no event shall the Supplier Process the Personal Data for its own purposes or those of any third party.

b. The Supplier guarantees that it shall implement and undertakes that it shall maintain appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the Agreement, this

Schedule and Data Protection Laws and to ensure the protection of the rights of the Data Subject.

c. The Supplier shall, and shall ensure that its employees, agents, contractors, sub-contractors and Sub-Processors shall, comply with all Data Protection Laws with regard to the provision of the Services and in the exercise of its respective rights and obligations under the Agreement and this Schedule.

d. The Supplier shall, and shall ensure that its employees, agents, contractors, sub-contractors and Sub-Processors shall, only Process Personal Data in accordance with the Company's documented instructions as set out in the Agreement or as notified by the Company to the Supplier in writing from time to time.

e. The Supplier shall immediately and, in any event, within forty eight (48) hours of becoming aware of the same, notify the Company if it is required by Applicable Law to act other than in accordance with the Company's instructions referred to in clause 5.1 (d).

f. The Supplier shall immediately (and not later than forty eight (48) hours) inform the Company if, in its reasonable opinion, it believes, that an instruction referred to in clause 5.1(d) infringes Data Protection Laws.

g. The Supplier acknowledges that the Company may assess the Data Processing contemplated by this Schedule against Applicable Laws, from time to time, whereupon notice from the Company, the Supplier shall promptly resolve any relevant issues identified by the Company and agreed by the Supplier as a breach or potential breach of such Applicable Laws or of the Supplier's obligations under this Schedule.

h. The Supplier shall ensure that in each case, processing and access to Personal Data is strictly limited to employees, agents, sub-processors and contractors, as authorised by the Supplier and who need to Process or access the relevant Personal Data, as is strictly necessary to perform the Services in the context of that person's duties to the Supplier (the "**Authorised Personnel**").

i. The Supplier shall ensure that any Authorised Personnel:

   i. have entered into an appropriate confidentiality agreement with the Supplier or are otherwise subject to a statutory obligation of confidentiality regarding the Personal Data;

   ii. are informed of the confidential nature of the Personal Data;

   iii. are subject to appropriate user authentication and log on processes when accessing Personal Data; and

   iv. have undertaken, and shall continue to receive, appropriate and regular training in relation to Data Protection Laws;

j. The Supplier shall, and shall ensure that its sub-processors shall, taking into account the nature of the Processing and the information available to the Supplier, assist the Company in ensuring compliance with its obligations under Applicable Laws, which shall include assisting with any Data Protection Impact Assessments and prior consultations conducted by the Company in accordance with Data Protection Laws.

k. Each of the parties acknowledge and agree that the Appendix attached hereto (Data Processing Details Form) is an accurate description of the Processing being carried out under the Agreement as at the Effective Date, including in relation to: (a) the subject matter, duration, nature and purpose of the Processing; (b) the type of Personal Data being Processed; and (c) the categories of Data Subjects. If the Processing changes as a result of receiving lawful written instructions from the Company, then the relevant Appendix must be updated by the Supplier. The Supplier shall only Process those categories of Personal Data that are described in relevant Data Processing Details Form and shall act in good faith to cooperate with any reasonable request by the Company to record additional details in the relevant Data Processing Details Form with respect to such categories of Personal Data.

5.2 **Sub-Processing**

a. The Supplier shall be authorised to engage third parties (each a "Sub-Processor") to Process Personal Data on behalf of the Company, provided that it notifies the Company, save where the Supplier is legally prohibited from notifying the Company.

b. The Company hereby specifically authorises the use of the Sub-Processors set out in the Data Processing Details Form of this Schedule.

c. The Company retains the right to review any Sub-Processors used by the Supplier and object to the use of any such Sub-Processors at any time should it reasonably believe that the Sub-Processor is not or may not continue to be compliant with Data Protection Laws. If such an objection is raised, the Parties shall use reasonable endeavours to resolve the objection in good faith. If the objection cannot be resolved, the objection shall either be withdrawn or the Company shall have the right to terminate the Agreement on written notice without penalty to either Party.

d. Where the Supplier does engage another Sub-Processor in accordance with 5.2.a above, the Supplier shall ensure that it has carried out appropriate due diligence on the Sub-Processor to ensure that it is capable of providing the level of protection to the Processing as is required by the Applicable Laws and this Schedule. The Supplier shall ensure that, from the Effective Date, any Sub-Processor engaged by the Supplier to process the Personal Data shall enter into an agreement with the Supplier on terms that are substantially the same as, but no less onerous than, the terms set out in this Schedule.

5.3 **International Data Transfers**

a. The Supplier shall not transfer Personal Data out of the European Economic Area (EEA) without the Company's express prior written authorisation, or unless required to do so under Applicable Laws, whereby the Supplier shall notify the Company of such a legal requirement prior to the Processing, save where the Supplier is legally prohibited from notifying the Company.

b. Any authorisation by the Company in accordance with 5.3 (a) shall be subject to the Supplier complying with relevant Data Protection Laws, including the implementation of the appropriate safeguards set out in Article 46.2 of the UK GDPR, into agreements with the applicable Sub-Processors (save where the UK Information Commissioner's Office has determined that

the third country or international organisation ensures an adequate level of protection in accordance with Article 45 of the UK GDPR).

c. Notwithstanding any other provisions of this Agreement, the Company hereby acknowledges the access and viewing by the Supplier's Group located in strategic worldwide locations strictly for the purposes of provision of continuous support to the Services (the "**Support Services**"), provided that:

   a. the Support Services are only provided by Group entities and do not involve any third parties;

   b. the Support Services do not involve any physical transfer of Personal Data, with occasional access provided to the Personal Data located in the EU or the United Kingdom, through secure means approved by the Group's Data Protection Officer;

   c. the access to Personal Data is only in support of situations where a problem ticket has been raised during out of normal working hours and local support is unavailable. Full logging occurs and such logs are stored within the EU and the United Kingdom;

   d. the Support Services provider shall comply with any published Group policy on data protection compliance, as amended from time to time;

   e. the Support Services provider shall comply with the IT Security and processing of Personal Data obligations imposed on the Supplier;

   f. all support personnel are under an obligation of confidentiality and have received (and shall continue to receive) appropriate training on data protection and privacy; and

   g. the Support Services provider shall not impose any restrictions on the rights or effective legal remedies of Data Subjects or the Company.

5.4 **Record Keeping**

a. The Supplier shall supply to the other Party all of the information set out in the Data Processing Details Form of this Schedule in order that the Company may retain a record of the Data Processing activities related to the Services.

b. The Supplier shall notify the Company prior to the implementation of any changes to its Data Processing activities relating to the Services except when such changes are carried out pursuant to the written instructions of the Company and, at the Company's cost, assist in carrying out any necessary Data Protection Impact Assessments.

c. The Supplier shall maintain its own records of its Data Processing activities relating to the Services, in accordance with Applicable Laws and shall make these records available to the Company on written request in a timely manner and subject to the Company's obligations of confidence set out in the Agreement. The Company shall be permitted to disclose such records to its professional advisors and applicable Regulators.

5.5 **IT Security**

a. The Supplier shall, at its own cost and expense, implement and maintain, appropriate technical and organisational measures to ensure a level of security:

i. Such that the Processing will meet the requirements of the Applicable Laws; and

j. Appropriate to the risks that are presented by the Processing.

b. The Supplier shall assist the Company in ensuring compliance with its obligations under Applicable Laws regarding the security of Processing and 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 the Data Subjects.

5.6 **Rights of the Data Subject**

a. The Supplier shall notify the other Party within three (3) working days if it receives: (a) from a Data Subject an actual or purported request exercising a Data Subject's rights (whether by the Data Subject or on its behalf) in accordance with Applicable Laws, including any one of: a request to access their Personal Data, rectify any inaccurate Personal data, have Personal Data erased, restrict the Processing of their Personal Data, obtain a portable copy of Personal Data or to transfer such a copy to a third party; an objection to any Processing of their Personal Data, or any other request, complaint or communication relating to obligations under Applicable Laws from a Data Subject (a "**Data Subject Request**"); or (b) requests, correspondence or communications (whether written or verbal) from a Regulator ("**Regulator Correspondence**").

b. The Supplier shall, without undue delay, provide the Company with full details of any Data Subject Request or Regulator Correspondence and reasonable details of the circumstances giving rise to it, including details of the relevant Personal Data or other information reasonably requested by the Company, which the Company shall be permitted to disclose to its professional advisors and applicable Regulators.

c. The Supplier shall provide all reasonable co-operation to allow the Company to investigate any such Data Subject Request or Regulator Correspondence and, taking into consideration the nature of the Processing, the Supplier shall assist the Company by appropriate technical and organisation measures, insofar as is possible, to enable the Company to fulfil its obligations to respond to such Data Subject Request or Regulator Correspondence. This should be coordinated with the Supplier's Data Protection Officer.

d. The Supplier shall not fulfil or respond to any Data Subject Request without first notifying the other Party.

e. The Supplier shall, and ensure that its authorised Sub-Processors shall, have in place appropriate technical and organisational measures to enable:

i. the proper rectification of inaccurate Personal Data either (i) in accordance with such a request from the Data Subject; or (ii) the other Party, duly authorised;

ii. the complete erasure, to the extent required by law, of a specified Data Subject's Personal Data; and

iii. the ability for individual Data Subject's Personal Data to be transported to the Data Subject or a third party, in a recognisable and commonly used format.

f. The actions set out under 5.6 (e) (i) - (iii) would only be undertaken by the Supplier or its Sub-Processors after specific written requests from the Company.

5.7 **Data Breach Notification**

a. Save where the Supplier is legally prohibited from notifying the Company, the Supplier shall notify the Company without undue delay and in any case within twenty-four (24) hours after becoming aware of any actual or suspected Personal Data Breach. Such notification shall:

i. Describe as far as is known to the Processor, the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects affected and the categories and approximate number of Personal Data records concerned;

ii. Communicate the name and contact details of the data protection officer or other point of contact where further information, if any, can be obtained;

iii. Describe the likely consequences of the Personal Data Breach;

iv. Describe the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

b. The Supplier acknowledges and understands that the Controller may be obligated to notify the relevant Regulators (within seventy-two (72) hours of having become aware of the Personal Data Breach) and may also be obligated to notify affected Data Subjects. The Processor shall provide all necessary assistance and relevant information reasonably requested by the other Party, in order to allow the Company to properly assess, investigate, mitigate and remedy the Personal Data Breach and to meet its respective obligations under Applicable Laws. Once the Supplier has notified the Company of any Personal Data Breach, the Supplier shall use its reasonable endeavours to not notify the relevant Regulators or the affected Data Subjects without obtaining the Company's prior approval. On request for approval, the Company shall not unreasonably delay or withhold approval where the Supplier is required under Applicable Law to notify a relevant Regulator of the Personal Data Breach.

5.8 **Audit**

a. The Company or a third party auditor appointed by the Company (the "Auditor") shall be permitted to conduct an audit once a year in normal circumstances subject to a ten (10) day notice period or at any time after a notified data breach subject to 5 days' notice period, in order for the Auditor to be satisfied that the Supplier is in compliance with its Processing obligations under this Schedule. Accordingly, the Auditor shall be permitted access to the Supplier's relevant premises, systems, records, processes and personnel, to the extent such access shall not result in the Supplier, as reasonably determined by the Supplier, breaching any Applicable Laws or confidentiality obligations with other third parties.

b. The Supplier shall reasonably co-operate, assist and make available to the Auditor all information necessary to demonstrate its compliance with its Processing obligations.

5.9 **Termination or Expiration of Processing Services**

a. In the event that the relevant Regulatory Authority determines and notifies the Supplier that it is not meeting its obligations with regards to the Processing of Personal Data relating to the Services, and no grace period is permitted by the Regulator Authority to remedy the issue, then the Company shall be entitled to terminate all impacted Services without penalty.

b. Upon the termination or expiration of the relevant Services, the Supplier shall at Company's option either (a) securely delete all Personal Data, including any copies, in such a manner that it cannot be recovered or reconstructed, unless Applicable Law requires storage of the Personal Data; or (b) return all Personal Data to Company by a technical means agreed by Company and securely delete existing copies in such a manner that they cannot be recovered or reconstructed, unless Applicable Laws require storage of such Personal Data.

c. The Supplier shall confirm to Company in writing that it has completed the actions prescribed in 5.9.a above.

APPENDIX TO ANNEX 1

DATA PROCESSING DETAILS FORM

Details regarding the Personal Data that is Processed by the Supplier that is provided by the Company:

1. The nature and purpose of the Processing (the "Subject Matter")

   The platform processes interactive communications on a mass scale and enables instant communications through any medium that can connect to an IP network. In addition it also has the capability to process call data via routing and recording facilities. This enables a Customer to process its client data in a consistent manner. It processes data provided by its' Customers with the specific nature and purpose of the processing being agreed with the Customer.
2. The Categories of Data Subjects

   Company's Customers
3. The type of Personal Data being Processed

   User data – any contact and authentications details of the Company's users
   Content data – including a range of personal data that is processed in the provision of the Services
4. The duration of the Processing (to include retention periods for the data)

   Term of the Agreement

5. The Categories of any recipients of the Personal Data (if any)

   None
6. Any transfers of the Personal Data outside of the EEA

   None
7. A general description of the technical and organisation security measures in place (or reference to an appropriate Information Security Schedule of the Agreement)

   We seek to hold all relevant accreditations as a means to demonstrate our commitment to quality, security and the environment. To this end we maintain a documented Business Management System that contains a number of Policies, Procedures and Work Instructions that support the following certifications:
   - ISO27001 Information Systems Management
   - ISO 9001 Quality Management
   - ISO 14001 Environmental Management
   - PCI DSS v3.2
   - Cyber Essentials

   To support this we also have in place a layered technical defence involving firewalls, access control, end point protection and a two factor authentication system for internal access to the platform.
8. Details of any Sub-Processors that you have engaged who are also Processing the Personal Data in the performance of the Services:

   Based on the Services, the Sub-Processors may be one or more of the following:
   - Redwood Technologies Limited

- Microsoft
- Teleopti AB
- Google
- IBM
- mGage
- Amazon