Data Processing Agreement

This data processing agreement including its schedules ("**DPA**") is supplemental to the Master Services Agreement ("**MSA**") and relates solely to matters relating to personal data that is processed by LoopUp Limited ("**LoopUp**") on behalf of the customer ("**Customer**"). Except where required to give proper interpretation to this DPA, the MSA shall not be amended. This DPA is entered into and takes effect as of the last date of the signatures of the parties.

1. Interpretation

1.1 In this DPA:

"**Data Protection Laws**" means all applicable laws, regulations, and requirements of regulatory guidance, in any applicable jurisdiction, relating to data protection, privacy and confidentiality of personal data, including the UK Data Protection Act 2018, European General Data Protection Regulation and any implementing, derivative or related legislation, rule, regulation, and regulatory guidance, as amended, extended and re-enacted from time to time, applicable to LoopUp;

"**Data Subject**" means an identifiable natural person of which the Customer is the data controller and LoopUp is data processor for the Customer, being an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**Personal Data**" means any information Processed by LoopUp where a Data Subject is identified or is identifiable;

"**Personal Data Breach**" means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed which results, or is likely to result, in a risk to the rights and freedoms of Data Subjects such as loss of control over their Personal Data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of Personal Data protected by professional secrecy or any other significant economic or social disadvantage to the Data Subject concerned;

"**Processing**", "**Process**" and "**Processed**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data as part of the provision of the Services to the Customer, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**Services**" has the meaning defined or as set out in the MSA;

"**Standard Contractual Clauses**" means the standard contractual clauses (Model Clauses) for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council and as amended from time to time; and

"**Sub-Processors**" has the meaning as set out in Schedules 2 and 3 to this DPA, as amended from time to time.

1.2 Headers are provided for convenience only and will not affect the interpretation of this DPA. In this DPA, a reference to: a person includes a reference to a natural or legal person and that person's successors and permitted assigns; the singular includes the plural, the masculine includes the feminine and vice versa; and 'writing' means any legible, visible and permanent form including hand-written and printed documents and electronic mail communications (including printed records thereof).

2. Personal Data and Processing

2.1 The Customer is the controller and LoopUp the processor in respect of all Personal Data made available to and Processed by LoopUp in connection with the provision of the Services for the term of the MSA.

2.2 A description of the types of Personal Data together with the nature, duration and purpose of the Processing activities are set out in Schedule 1 to this DPA.

2.3 LoopUp will Process the Personal Data solely in accordance with the written instructions of the Customer including such instructions as set out in this DPA and in such manner as is necessary for the purposes of the provision of the Services pursuant to the MSA (unless required to do so otherwise by law or regulation applicable to LoopUp or the Customer).

2.4 LoopUp shall not Process the Personal Data for any other purpose other than as set out in clause 2.3 or in a way that does not comply with this DPA or the Data Protection Laws. LoopUp shall notify the Customer if, in its opinion, the Customer's instruction would not comply with Data Protection Laws.

2.5 LoopUp shall promptly comply with any Customer reasonable request or instruction requiring LoopUp to amend, transfer, delete or otherwise Process the Personal Data, or to stop, mitigate or remedy any unauthorised Processing. Such instructions shall not unnecessarily restrict the provision of Services (and billing thereof).

2.6 Where the Customer is providing Personal Data to LoopUp to Process in accordance with this DPA, it confirms that it has the requisite authority to do so as data controller.

3. Security Measures

3.1 LoopUp shall ensure that all employees of LoopUp that Process Personal Data pursuant to the MSA:

a) are informed of the confidential nature of the Personal Data and are subject to suitable confidentiality obligations;

b) undertake training on the Data Protection Laws and how the obligations relating to data protection apply to their duties; and

c) are aware of their duties pursuant to this DPA.

3.2 LoopUp shall implement appropriate technical and organisational measures (including those as set out in Schedule 2 to this DPA) to ensure a level of security appropriate to the risks presented by the Processing, including, but not limited to, as appropriate:

d) the pseudonymisation and encryption of Personal Data;

e) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

f) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

g) a process for routinely testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

4. Confidentiality and Sub-Processors

4.1 LoopUp shall maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless authorised by the Customer or permitted pursuant to this DPA, the MSA or as required by law. If a law, court, regulator or supervisory authority requires LoopUp to Process or disclose Personal Data, LoopUp must first inform the Customer of the legal or regulatory requirement and provide the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

4.2 LoopUp shall be authorised to appoint:

a) specifically – the Sub-Processors to Process Personal Data on behalf of LoopUp; and

b) generally – such other processors as may be required from time to time in order to provide the Services, provided that LoopUp shall inform the Customer of any material changes affecting the Processing of Personal Data relating to the Services.

4.3 When appointing a Sub-Processor, LoopUp shall do so by way of a contract or other legal act to provide sufficient guarantees to implement appropriate technical and organisational measures to comply with the Data Protection Laws.

4.4 LoopUp shall be fully responsible for all acts or omissions of its employees, agents, and subcontractors (including the Sub-Processors) in the same manner as for its own acts or omissions in accordance with the Data Protection Laws.

5. Further assistance

5.1 LoopUp shall provide such assistance to the Customer:

a) as reasonably necessary for the Customer to meet its obligations in respect of Data Subject rights under the Data Protection Laws;

b) as reasonably requested in performing, where required, a data protection impact assessment, and in consulting with competent authorities; and

c) notifying the Customer of any changes to the Data Protection Laws that may adversely affect LoopUp's performance of this DPA.

6. Notification

6.1 LoopUp shall notify the Customer, without undue delay, of:

a) discovering a Personal Data Breach, in which case LoopUp shall (i) as part of such notification describe the nature of the incident and, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, and (ii) investigate such Personal Data Breach and take such appropriate corrective action to remedy such breach and prevent a recurrence of such breach;

b) any request for information from or complaint by a data protection authority specifically in relation to Personal Data that LoopUp Processes for the purpose of providing the Services; and

c) any request to LoopUp by a Data Subject to exercise rights under the Data Protection Laws such as to access, rectify, amend, correct, share, delete or cease Processing their Personal Data.

7. Deletion of Personal Data

7.1 Except where permitted by any applicable law or regulation or as set out in, or as required pursuant to, the MSA, upon the request of the Customer, LoopUp shall delete or return all Personal Data to the Customer after the provision of the Services and completion of any accounting or administrative requirements relating to the provision of the Services.

8. International transfers

8.1 LoopUp and its Sub-Processors shall Process Personal Data only at locations and/or geographies outside of the European Economic Area provided the transfer is:

a) to a jurisdiction deemed by the European Commission to have an adequate level of protection;

b) subject to contractual provisions approved by the European Commission such as, by way of example only, the Standard Contractual Clauses; or

c) pursuant to a framework deemed adequate and approved by the European Commission.

9. General

9.1 This DPA may be executed in any number of counterparts, and by each party on separate counterparts. Each counterpart shall be deemed to be an original, but all counterparts shall together constitute one and the same instrument.

9.2 To the extent there is no conflict, the terms of the MSA shall apply to the interpretation of this DPA.

9.3 This DPA 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.

9.4 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 DPA or its subject matter or formation.

Signed for and on behalf of **LoopUp**	Signed for and on behalf of the **Customer**
By:	By:
Signature:	Signature:
Date:	Date:

Schedule 1 – Processing

Categories of Data Subjects	Users of the Services.
Categories of Personal Data	The following categories of Personal Data may be Processed by LoopUp: a) name, email, phone number (desk and mobile) and office location of users of the Services (which may include employees, partners and clients of the Customer); b) contact details of account administrators and employees of the Customer; c) call detail records of users (such as call duration and time) as may be required for the administration and delivery of the Services; d) call recordings as may be performed as part of the Services; and e) such other Personal Data as required or ancillary to provide the Services. LoopUp has no knowledge or intertest in the Personal Data transmitted through, stored on or accessed from the LoopUp system (i.e. content of calls) and other than to monitor performance of the LoopUp systems has no duty to monitor any content made available or published through the LoopUp systems.
The frequency of the transfer	For the duration of the provision of the Services.
Nature of the Processing	For the provision of the Services (telecommunication services).
Purpose of the data transfer	Performance of LoopUp's obligations pursuant to the MSA (including the provision of the Services).
Retention period	For the duration of the provision of (and billing of) the Services.
Sub-processors	As set out in Schedule 3 and such other third party organizations that may help provide, run and manage internal IT systems or provide additional support (such as credit agencies, professional advisers or where LoopUp agrees to provide additional services (such as operator assisted event calls or where payment by credit card is permitted and may be processed by a PCI-DSS compliant third party provider)).

Schedule 2 – Technical and Organisational Measures

LoopUp must ensure that the latest standards for security and data protection are met and exceeded for the Services, including the protection of personal and confidential data. These standards include operating an information security management system (ISMS) in accordance with the ISO 27001:2013 standard.

LoopUp commits to on-going, comprehensive investments in hardware and software solutions, current technologies and associated processes, policies and audits to ensure that the protective measures are complied with and continually improved.

1 Access Control (Building / Offices / Data Centre)

1.1 LoopUp has implemented measures to prevent the unauthorised access to data processing systems where personal data is processed including, where appropriate and without limitation, the following:

(a) Alarm system

(b) Automatic access control system

(c) Photoelectric sensors / movement detectors (for alarm system)

(d) Key Management (Issuance of keys, etc.)

(e) Visitor management at reception desks

(f) Protection of building shafts

(g) Manual locking system (limited usage for key employees to be used in the event of a failure in the access control systems)

(h) CCTV at entry points (office and data centres)

(i) Security locks

(j) Careful selection of cleaning staff

(k) A separate, specific and documented access control for data centres and server rooms for authorised persons is implemented. Access by authorised persons is documented by name and card or token number. For the data centres, separate access control systems are implemented.

2 Access Control (Systems)

2.1 LoopUp has implemented measures to prevent the use of data processing systems by unauthorised persons including, without limitation, the following:

(a) Assignment of user rights

(b) Assignment of passwords

(c) Authentication with username / password

(d) Use of Intrusion-Prevention-Systems

(e) Use of Hardware Firewalls

(f) Creation of user profiles

(g) Additional measures: web-application firewalls, regular vulnerability scans, regular penetration testing, patch management, minimum requirements for password complexity and forced password changes, use of virus scanners

(h) Assignment of user profiles to IT systems

(i) Use of VPN Technology

(j) Encryption of mobile storage media

(k) Use of central smartphone administration (for example: remote wiping of smartphone)

(l) Use of a software firewall (office clients)

3 Access Control (Data)

3.1 LoopUp has implemented measures to ensure that authorised users of a data processing system may only access the data for which they are authorised, and to prevent personal data from being read while the data is in use, in motion, or at rest without authorisation including, without limitation, the following:

(a) Creation of an authorisation concept

(b) Number of administrators reduced to "absolute necessary"

(c) Logging of application access, especially during the entry, modification and deletion of data

(d) Secure media sanitisation before re-use

(e) Use of shredders or services (if possible with privacy seal)

(f) Disk encryption (backup tapes for off-site storage)

(g) Management of rights by system administrators

(h) Password policy including password length, password change management

(i) Secure storage of data carriers

(j) Logging of secure media destruction

(k) Compliant destruction of data media

4 Transfer Control

4.1 LoopUp has implemented measures to ensure that personal data cannot be read, copied or modified during electronic transmission or during transportation or storage to disk, additionally to control and determine to which bodies that the transfer of personal data provided by data communication equipment is allowed including, without limitation, the following:

(a) Creation of dedicated lines or VPN tunnels

(b) Documentation of recipients of data and the time periods for the provision of data including agreed deletion times

(c) During physical transport, careful selection of transport personnel and vehicles (tape off-site storage)

(d) Disk encryption (backup tapes for off-site storage)

(e) Disclosure of data in anonymous or pseudonymous form

(f) TLS encryption of all communications (Web-Client, APIs, mobile Apps)

5 Input Control

5.1 LoopUp has implemented measures to ensure that it is possible to ensure, subsequently control, and determine if and by whom, personal data has been entered, changed or removed on data processing systems including, without limitation, the following:

(a) Logging of input, modification and deletion of data

(b) Traceability of input, modification and deletion of data by individual user names (not user groups)

(c) Granting of rights for the input, modification or the deletion of data based on an authorisation concept

(d) Creation of an overview of which applications are permitted to input, modify or delete which data

(e) Storage of forms, through which data has been acquired during automated processing

6 Order Control

6.1 LoopUp has implemented measures to ensure that personal data which is processed by request of the data owner by a data processor, shall only be processed as instructed including, without limitation, the following:

(a) Subcontractor selection via history review (in particular regarding data security)

(b) Written instructions to the Subcontractor (for example, by Data Processing Agreement)

(c) Effective control rights over data processors have been agreed

(d) Prior examination of the documentation and the security measures taken by the Subcontractor

(e) Obligation of the Subcontractors' employees to maintain data confidentiality

(f) Ensure the secure destruction of data after termination of the contract

(g) Continual review of Subcontractor and their activities

7 Availability Control

7.1 LoopUp has implemented measures to ensure that personal data is protected against accidental destruction or loss including, without limitation, the following:

(a) Uninterruptible power supplies (UPS)

(b) Devices for monitoring temperature and humidity in server rooms

(c) Fire and smoke detection systems

(d) Alarm when unauthorised entry to server rooms is detected

(e) Testing of data recovery

(f) Secure off-site storage of data backups

(g) In flood areas, server rooms are above the water border

(h) Air conditioning in server rooms

(i) Protection power strips in server rooms

(j) Fire extinguishers in server rooms

(k) Creation of a backup & recovery concept

(l) Preparation of an emergency response plan

(m) Server rooms not located under sanitary installations

8 Segregated Processing

8.1 LoopUp has implemented measures to ensure that data which is collected for different purposes can be processed separately including, without limitation, the following:

(a) Creation of an authorisation concept

(b) Provision of records with purpose attributes / data fields

(c) Approved and documented database rights

(d) Logical client separation (in software)

(e) In pseudonymous data: the separation of the mapping file and storage on a separate secured IT system

(f) Separation of production and test systems

Schedule 3 – List of Sub-Processors

LoopUp shall only share data with third parties when legally permitted to do so and in accordance with this DPA. Such Sub-Processors shall include:

Sub-Processor	Processing activity	Safeguards
Salesforce	Managing LoopUp CRM	Standard Contractual Clauses/ data processing agreement and security review
Microsoft	Communications and storage of limited amounts of data	Standard Contractual Clauses/ data processing agreement and security review
SendGrid	Delivery of secure email communications	Standard Contractual Clauses/ data processing agreement and security review
Mixpanel	Customer support management	Standard Contractual Clauses/ data processing agreement and security review
Kansys	Billing	Standard Contractual Clauses/ data processing agreement and security review
Other members within the LoopUp group of companies	For the provision of Services to Customer (namely customer support)	Standard Contractual Clauses (falls within LoopUp internal and external security reviews)

Data centres
LoopUp provides its services from regional datacentres located in the United States (Chicago, Miami), Europe (London), Asia (Hong Kong) and Australia (Sydney). Each datacentre is collocated with industry-leading hosting partners and positioned strategically to be at the centre of multiple Tier 1 telephony and data service providers enabling LoopUp to deliver highly available, high quality, cost effective services. Within each datacentre, LoopUp's infrastructure is designed to maximise availability and service performance.

Carriers
Calls are delivered to and from LoopUp's datacentres via resilient connections to multiple Tier-1 carriers using both circuit-switched telephony (PSTN) and packet-switched telephony (VoIP) over managed Quality-of-Service networks. Carriers are selected primarily based on quality, which is continually monitored. LoopUp works with Tier-1 carriers that have extensive global or regional networks that keeps calls 'on-net' as close as possible to local providers.