DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") applies to Sendible Limited (company number 06815657) ("Sendible") and its processing of Personal Data in relation to the provision of Sendible's Services to you, the Customer. Unless otherwise expressly stated in the Agreement, this DPA shall be effective and remain in force for the full term of the Agreement. Sendible and the Customer each may be referred to herein as a "Party" or collectively as the "Parties."

1 DEFINITIONS

1.1 "Agreement" means the Terms of Service located at https://www.sendible.com/terms or a contract referencing this DPA under which Sendible has agreed to provide Services.

1.2 "Applicable Data Protection Legislation" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time.

1.3 "Controller" will have the following meaning (as applicable): (a) the meaning given to "controller" under Applicable Data Protection Legislation; or (b) the meaning given to "business" under Applicable Data Protection Legislation.

1.4 "Covered Data" means Personal Data shared by Customer or a Customer Affiliate in relation to the provision of the Services.

1.5 "Customer" means "you" or the party with whom Sendible provides Services under the Agreement.

1.6 "Customer Affiliate" means an affiliate of Customer who is a beneficiary to the Agreement.

1.7 "Data Subject" means a natural person whose Personal Data is part of the Covered Data.

1.8 "Data Subject Requests" means a request from a Data Subject to exercise their rights under Applicable Data Protection Legislation. "GDPR" means Regulation (EU) 2016/679.

1.9 "Personal Data" means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise "personal data," "personal information," "personally identifiable information," or similarly defined data or information under Applicable Data Protection Legislation.

1.10 "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means. "Process", "Processes" and "Processed" will be interpreted accordingly.

1.11 "Processor" will have the following meaning (as applicable): (a) the meaning given to "processor" under Applicable Data Protection Legislation; or (b) the meaning given to "service provider" under Applicable Data Protection Legislation.

1.12 "Security Incident" means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Covered Data.

1.13 “Services” means the services to be provided by Sendible pursuant to the Agreement.

1.14 “Standard Contractual Clauses” or “SCCs” means Module Two (controller to processor) and/or Module Three (processor to processor) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.

1.15 "Subprocessor" means an entity appointed by Sendible, as a Processor, to Process Covered Data on its behalf.

1.16 “UK GDPR” has the meaning given under the Data Protection Act 2018 (UK).

2 GENERAL. This DPA is incorporated into and forms an integral part of the Agreement. If there is any conflict between this DPA and the Agreement relating to the Processing of Covered Data, this DPA shall govern. Customer acknowledges and agrees that Sendible may amend this DPA from time to time on reasonable notice to Customer where such changes are required because of changes in Applicable Data Protection Legislation.

3 SENDIBLE OBLIGATIONS AS PROCESSOR

3.1 Where Sendible is processing Personal Data for Customer as a processor, Sendible will:

3.1.1 only do so on documented Customer instructions and in accordance with the Applicable Data Protection Legislation, including with regard to transfers of Personal Data to other jurisdictions or an international organization, and the parties agree that the Agreement constitutes such documented instructions of the Customer to Sendible to process Personal Data (including to locations outside of the relevant jurisdiction) along with other reasonable instructions provided by the Customer to Sendible (e.g. via email) where such instructions are consistent with the Agreement;

3.1.2 ensure that all Sendible personnel involved in the processing of Personal Data are subject to confidentiality obligations in respect of the Personal Data;

3.1.3 make available information necessary for Customer to demonstrate compliance with its applicable obligations under Data Protection Legislation where such information is held by Sendible and is not otherwise available to Customer through its account and user areas or on Sendible websites, provided that Customer provides Sendbile with at least 14 days' written notice of such an information request;

3.1.4 co-operate as reasonably requested by Customer to enable Customer to comply with any exercise of rights by a Data Subject afforded to Data Subjects by Data Protection Legislation in respect of Personal Data processed by Sendible in providing the Services;

3.1.5 upon deletion by Customer, not retain Personal Data from within Customer’s account other than in order to comply with Applicable Data Protection Legislation and as may otherwise be kept in routine backup copies made for disaster recovery and business continuity purposes subject to Sendible’s retention policies;

3.1.6 cooperate with any regulator in the performance of such regulator’s tasks where required;

3.1.7 assist Customer as reasonably required where Customer:

3.1.7.1 conducts a data protection impact assessment involving the Services (which may include by provision of documentation to allow Customer to conduct such assessment); or

3.1.7.2 is required to provide notice of a Security Incident to a regulator or to a relevant Data Subject.

3.1.8 will not (a) sell any Personal Information (as defined under the Applicable Data Protection Legislation) for a commercial purpose, (b) collect, retain, use, disclose, or otherwise process Personal Information other than (1) to fulfill its obligations to Customer under the Agreement, (2) on the Customer's behalf, (3) for the Customer's operational purposes, (4) for Sendible's internal use as permitted by Applicable Data Protection Legislation, (5) to detect data security incidents or protect against fraudulent or illegal activity, or (6) as otherwise permitted under Applicable Data Protection Legislation, or (c) limit sharing of Personal Information when requested by a consumer or data subject; and

3.1.9 will inform Customer if it comes to its attention that any instructions received by Customer infringe the provisions of Applicable Data Protection Legislation. Notwithstanding the foregoing, Sendible shall have no obligation to monitor or review the lawfulness of any instruction received from the Customer.

4 SUBPROCESSORS

4.1 Customer grants Sendible the general authorization to engage Subprocessors listed in Schedule 4, and any additional Subprocessors in accordance with Section 4.3.

4.2 Sendible will: (i) enter into a written agreement with each Subprocessor imposing data protection obligations that are substantively no less protective of Covered Data than Sendible's obligations under this DPA; and (ii) remain liable for each Subprocessor's compliance with the obligations under this DPA.

4.3 In the event that Sendible wishes to appoint an additional Sub-processor: (a) Sendible will provide Customer reasonable notice; and (b) Customer may, on the basis of reasonable data privacy and data security concerns, object to Sendible's use of such Subprocessor by providing Sendible with written notice of the objection within ten (10) days of the date of such notice, otherwise the additional Subprocessor shall be deemed approved. In the event Customer objects to Sendible's use of a new Subprocessor, Customer and Sendible will work together in good faith to find a mutually acceptable resolution to address any objections raised by Customer.

5 DATA SUBJECT RIGHTS REQUESTS

5.1 Sendible will forward to Customer promptly any Data Subject Request received by Sendible relating to the Covered Data and may advise the Data Subject to submit their request directly to Customer.

5.2 Sendible will, taking into account the nature of the Processing of Covered Data, provide Customer with reasonable assistance as necessary for Customer to fulfil its obligation under Applicable Data Protection Legislation to respond to Data Subject Requests.

6 SECURITY

6.1 Sendible has designed a commercially reasonable information security program that incorporates technical, administrative and organizational measures (in accordance with Schedule 2, attached hereto) that provide a level of security appropriate to the level of risk of possible unauthorized or unlawful processing, accidental loss of and/or damage to Personal Data..

6.2 Sendible will notify Customer in writing without undue delay after becoming aware of any Security Incident. Sendible will, to the extent reasonably necessary, cooperate with Customer's investigation of the Security Incident. Sendible's notification of, or response to, a Security Incident will not be construed as an acknowledgement by Sendible of any fault or liability with respect to the Security Incident.

7 AUDITS AND RECORDS

7.1 Upon request, Sendible will make available to Customer information reasonably necessary to demonstrate compliance with this DPA.

7.2 To the extent required by Applicable Data Protection Legislation, Sendible will permit Customer (or a suitably qualified, independent third-party auditor which is not a competitor of Sendible) to audit Sendible's compliance with this DPA no more than once per calendar year on at least thirty (30) days' written notice to Sendible (an "Audit"), provided that Customer (or Customer's third-party auditor, as applicable):

7.2.1 may only conduct an Audit during Sendible's normal business hours;

7.2.2 will conduct the Audit in a manner that does not disrupt Sendible's business;

7.2.3 enters into a confidentiality agreement reasonably acceptable to Sendible prior to conducting the Audit;

7.2.4 pays any reasonably incurred costs and expenses incurred by Sendible in the event of an Audit;

7.2.5 ensures that its personnel comply with any policies and procedures notified by Sendible to Customer when attending Sendible's premises;

7.2.6 submits, as part of the written notice provided by Customer to Sendible, a detailed proposed audit plan which is agreed by Sendible (an "Audit Plan"); and

7.2.7 conducts the Audit in compliance with the final agreed Audit Plan.

7.3 Customer may use the results of an Audit only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of the DPA. Nothing in this Section 7 will require Sendible to breach any duties of confidentiality it owes to third parties.

8 TRANSFER OF COVERED DATA

8.1 Where the transfer of Covered Data to Sendible is a Restricted Transfer, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form an integral part of the Agreement in accordance with Schedule 3 of this DPA.

8.2 If and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Covered Data to Sendible, the parties shall reasonably cooperate to agree and take any actions that may be reasonably required to implement any additional measures or alternative transfer mechanism to enable the lawful transfer of such Covered Data. Additionally, in the event Sendible adopts an alternative transfer mechanism, such alternative transfer mechanism shall apply instead of the SCCs described in Section 8.1 of this DPA (but only to the extent such alternative transfer mechanism complies with Applicable Data Protection Legislation and extends to the territories to which Covered Data is transferred).

9 DELETION AND RETURN

9.1 Sendible will, in any event, within thirty (30) days of the date of termination or expiration of the Agreement (a) if requested to do so by Customer within that period, return a copy of all Covered Data or provide a self-service functionality allowing Customer to do the same; and (b) delete all other copies of Covered Data Processed by Sendible or any Subprocessors. It is the Customer’s responsibility to backup any Covered Data.

10 STANDARD CONTRACTUAL CLAUSES

10.1 The Parties agree that, to the extent required by Applicable Data Protection Legislation, the terms of the Standard Contractual Clauses Module 1 (Controller to Controller), Module Two (Controller to Processor) and/or Module Three (Processor to Processor),each as further specified in Schedule 3 of this DPA, are hereby incorporated by reference and will be deemed to have been executed by the Parties.

10.2 To the extent required by Applicable Data Protection Legislation, the jurisdiction-specific addenda to the Standard Contractual Clauses set out in Schedule 3 are also incorporated herein by reference and will be deemed to have been executed by the Parties.

10.3 To the extent that there is any conflict between the terms of this DPA and the terms of the Standard Contractual Clauses, the Standard Contractual Clauses shall govern.

10.4 Sendible will provide Customer reasonable support to enable Customer’s compliance with the requirements imposed on international transfers of Covered Data. Sendible will, upon Customer’s request and at Customer’s cost, provide information to Customer which is reasonably necessary for Customer to complete a transfer impact assessment ("TIA") to the extent required under Applicable Data Protection Legislation.

DATA PROCESSING ADDENDUM

SCHEDULE 1 - DETAILS OF PROCESSING AND TRANSFERS

1. PART A – List of Parties: The Parties are set out in the preamble to this DPA. With regard to any transfers of Covered Data falling within the scope of Applicable Data Protection Legislation, additional information regarding the data exporter and data importer is set out below.

    a. Data Exporter: The data exporter is: Customer and/or Customer Affiliates exporting Covered Data to which the GDPR applies. The data exporter's contact person's name, position and contact details as well as (if appointed) the data protection officer's name and contact details and (if relevant) the representative's contact details are included in the Agreement or will be disclosed to Sendible upon request.

    b. Data Importer: The data importer is: Sendible Limited, a company registered in England and Wales and our registered office is at 3rd Floor, 311 Ballards Lane, London, N12 8LY. The data importer's contact person and contact details are included in the Agreement or will be disclosed to Customer upon request.

2. PART B – Description of Processing

    a. Categories of Data Subjects - Determined by Customer (in accordance with the Agreement).

    b. Categories of Personal Data - Determined by the Customer (in accordance with the Agreement).

    c. Special categories of Personal Data (if applicable) - None.

    d. Duration and Frequency of the Processing - The Processing is performed on a continuous basis for the duration of the Agreement and is determined by Customer's configuration of the Services.

    e. Subject matter and nature of the Processing - Performing the Services on behalf of Customer which involves Processing (including collection, storage, organization and structuring) of Personal Data as part of our social media management Services, as further described in the Agreement; undertaking activities to verify or maintain the quality of the Services; debugging to identify and repair errors that impair existing intended functionality; helping to ensure security and integrity of the Services.

f. Purpose(s) of the data transfer and further Processing - To provide the Services to Customer pursuant to the Agreement and as may be further agreed upon by Customer and Sendible.

g. Storage Limitation - The duration is the term of the Agreement.

h. Subprocessor (if applicable) - To provide Processing system capability to Customer to provide the Services described in the Agreement.

3. PART C – Competent Supervisory Authority

a. Identify the competent supervisory authority/ies in accordance with clause 13 of the SCCs.

b. Where the data exporter is established in an EU Member State: The supervisory authority of the country in which the data exporter established is the competent authority.

c. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The competent supervisory authority is the one of the Member State in which the representative is established.

d. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without, however, having to appoint a representative pursuant to Article 27(2) of the GDPR: The competent supervisory authority is the supervisory authority of Ireland.

DATA PROCESSING ADDENDUM

SCHEDULE 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

1. Sendible has implemented the following technical and organizational measures (including any relevant certifications) to ensure an appropriate level of security, accounting for the nature, scope, context, and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

    a. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of Sendible's information security program.

    b. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Sendible's organization, monitoring and maintaining compliance with Sendible's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

    c. Utilization of commercially available and industry standard encryption technologies for Covered Data that is being transmitted by Sendible over public networks (i.e., the Internet) or when transmitted wirelessly.

    d. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).

    e. Password controls designed to manage and control password strength and usage including prohibiting users from sharing passwords and requiring that Sendible's passwords that are assigned to its employees.

    f. System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

    g. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Sendible's possession.

h. Change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Sendible's technology and information assets.

i. Incident / problem management policies and procedures designed to allow Sendible to investigate, respond to, mitigate, and notify of events related to Sendible's technology and information assets.

j. Network security controls that provide for the use of firewall systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

k. Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.

l. Business resiliency/continuity plan and procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

m. Vendor management for the review and assessment of risk of vendors according to the sensitivity of information such vendors have access to.

SCHEDULE 3 - STANDARD CONTRACTUAL CLAUSES (Modules 2 and 3)

1. Subject to Section 8.1 of the DPA, where the transfer of Covered Data to Sendible is a Restricted Transfer and Applicable Data Protection Legislation requires that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form part of the DPA as follows:

    a. In relation to transfers of Covered Data protected by the EU GDPR, the SCCs shall apply as follows:

        I. Module Two terms shall apply (where Customer is the controller of Customer Personal Data) and the Module Three terms shall apply (where Customer is the processor of Customer Personal Data);

        II. in Clause 7, the optional docking clause shall apply and Authorized Affiliates may accede the SCCs under the same terms and conditions as Customer, subject to mutual agreement of the parties;

        III. in Clause 9, option 2 ("**general authorization**") is selected, and the process and time period for prior notice of Sub-processor changes shall be as set out in Section 4.3 of the DPA;

        IV. in Clause 11, the optional language shall not apply;

        V. in Clause 17, option 1 shall apply and the SCCs shall be governed by Irish law;

        VI. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

        VII. Annex I shall be deemed completed with the information set out in Schedule 1 to the DPA; and

        VIII. Annex II shall be deemed completed with the information set out in Schedule 2 of the DPA.

    b. In relation to transfers of Covered Data protected by the UK GDPR, the SCCs as implemented under Section 1(a) above shall apply with the following modifications:

I. the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the DPA;

II. Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Schedule 1 and Schedule 2 to the DPA, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party"; and

III. Any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

c. In relation to transfers of Covered Data protected by the Swiss Data Protection Act, the SCCs as implemented under Section 1(a) above will apply with the following modifications:

I. references to “Regulation (EU) 2016/679” and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;

II. references to “EU”, “Union”, “Member State” and “Member State law” shall be replaced with references to “Switzerland” and/or “Swiss law” (as applicable);

III. references to the “competent supervisory authority” and “competent courts” shall be replaced with references to the “Swiss Federal Data Protection Information Commissioner” and “applicable courts of Switzerland”);

IV. the SCCs shall be governed by the laws of Switzerland ; and

V. disputes shall be resolved before the competent Swiss courts.

2. Where the Standard Contractual Clauses apply pursuant to Section 8.1 of this DPA, this section sets out the parties' interpretations of their respective obligations under specific provisions of the Clauses, as identified below. Where a party complies with the interpretations set out below, that party shall be deemed by the other party to have complied with its commitments under the Standard Contractual Clauses:

a. where Customer is itself a processor of Covered Data acting on behalf of a third-party controller and Sendible would otherwise be required to interact directly with such third party controller (including notifying or obtaining authorizations from such third party controller), Sendible may interact solely with Customer and Customer shall be responsible for forwarding any necessary notifications to and obtaining any necessary authorizations from such third party controller;

b. the certification of deletion described in Clause 16(d) of the SCCs shall be provided by Sendbile to Customer upon Customer's written request;

c. for the purposes of Clause 15(1)(a) the SCCs, Sendible shall notify Customer and not the relevant Data Subject(s) in case of government access requests, and Customer shall be solely responsible for notifying the relevant Data Subjects as necessary; and

d. Taking into account the nature of the processing, Customer agrees that it is unlikely that Sendible would become aware of Personal Data processed by Sendible is inaccurate or outdated. To the extent Sendible becomes aware of such inaccurate or outdated data, Sendible will inform the Customer in accordance with Clause 8.4 SCCs.

SCHEDULE 4 - SUBPROCESSORS

1. Sendible’s list of Subprocessors is available in our Privacy Policy: https://www.sendible.com/privacy

DATA PROCESSING ADDENDUM

Signed by the Customer:

Company name: _____

Name: _____

Title: _____

Date: _____

Signature: _____

Signed by Sendible:

Name: _____

Title: _____

Date: _____

Signature: _____