DATA PROCESSING ADDENDUM
TO INTERMEDIA'S MASTER SERVICE AGREEMENT

This Data Processing Addendum, including its Schedules and Exhibits, (collectively, the "**Addendum**") completes and forms part of Intermedia's Master Service Agreement available at https://www.intermedia.com/legal (or, for customers purchasing Services from Intermedia's U.K. subsidiary Intermedia Technologies Company Ltd., at https://www.intermedia.co.uk/legal), in each case as updated from time to time, or other agreement between Customer (as defined below) and Intermedia (as defined below) governing Customer's use of the Service (altogether "**Service Agreement**"). This Addendum is concluded between Intermedia.net, Inc., and its affiliates, subsidiaries and branches (collectively, "**Intermedia**") and each Customer that has agreed to the Service Agreement) ("**Customer**") and is subject to the terms, conditions, restrictions and limitations set forth in the Service Agreement.

This Addendum regulates the Processing of Personal Data subject to Data Protection Law (as defined in Section 2) for the Purposes (as defined in Exhibit C to Schedule 1) by the parties in the context of the Intermedia Service. The terms used in this Addendum have the meaning set forth in this Addendum. Capitalized terms not otherwise defined herein have the meaning given to them in the Service Agreement. Except as modified below, the Service Agreement remains in full force and effect. The Schedules and Exhibits to this Addendum form an integral part of this Addendum.

This Addendum contains the following sub-sections, Schedules and Exhibits set forth below:

<table>
<tr>
<td>Data Protection Terms

Section 1: How to Execute this Addendum
Section 2: Definitions
Section 3: Roles of the Parties
Section 4: Compliance with Data Protection Law
Section 5: Obligations of Customer
Section 6: Obligations of Intermedia
Section 7: Security of the Processing, Confidentiality, and Personal Data Breach Notification
Section 8: International Data Transfers
Section 9: Intermedia's Sub-Processing
Section 10: Data Protection and Security Audit
Section 11: Liability Towards Data Subject
Section 12: Applicable Law and Jurisdiction
Section 13: List of Schedules
Section 14: Modification of this Addendum
Section 15: Termination
Section 16: Invalidity and Severability</td>
<td>Schedule 1: EEA Region Specific Terms
• Exhibit A: Standard Contractual Clauses ("SCCs")
• Exhibit B: Annex I(A) to SCCs (List of Parties)
• Exhibit C: Annex I(B) to SCCs (Description of Transfer)
• Exhibit D: Annex I(C) to SCCs (Competent Supervisory Authority)
• Exhibit E: Annex II to SCCs (Technical and Organizational Measures)
• Exhibit F: Annex III to SCCs (List of Sub-Processors)

Schedule 2: California Consumer Privacy Act ("CCPA") Specific Terms

Schedule 3: United Kingdom Specific Terms</td>
</tr>
</table>

1. **How to Execute this Addendum.** This Addendum, as incorporated by reference into the Service Agreement between Intermedia and the Customer, is legally binding and automatically applies to all customers; provided, however, to the extent that Customer is located in a country that requires this Addendum to be executed by both parties, the Customer shall complete this Addendum by (a) logging into the Customer's administrative control panel for Intermedia services (e.g., HostPilot) and submitting a request to Intermedia in a manner made available under the Legal section of the administrative control panel and (b) electronically signing this Addendum in a manner provided by Intermedia (which may be in the form of an invitation sent by Intermedia or a link to an electronically executable version of this Addendum made available by Intermedia).

2. **Definitions**. The following terms have the meanings set out below for this Addendum:

2.1. "CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

2.2. "Confidential Data" means "Confidential Information" as defined by the Service Agreement.

2.3. "Controller" means the entity which determines the purposes and means of the Processing of Personal Data as defined by applicable Data Protection Law.

2.4. "Data Protection Law" means all laws and regulations applicable to the Processing of Personal Data under this Addendum, including without limitation the laws and regulations of the European Union, the EEA and their member states, Switzerland, the United Kingdom, Canada, Australia, Japan, and the United States and its states, as they each may be amended from time to time.

2.5. "Data Subject" means the identified or identifiable person to whom Personal Data relates.

2.6. "EEA" means the European Economic Area.

2.7. "Europe" means the EEA, the United Kingdom and Switzerland.

2.8. "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), as it may be amended from time to time.

2.9. "International Data Transfer" means any transfer of Personal Data from a country whose laws restrict international data transfer (the "Transferring Country") to an international organization or to a country outside of the Transferring Country (the "Receiving Country"), and includes any onward transfer of Personal Data from the international organization or the Receiving Country to another international organization or to another country outside of the Receiving Country.

2.10. "Personal Data" means any information relating to an identified or identifiable natural person.

2.11. "Personal Data Breach" means (i) any confirmed theft, loss or unauthorized use or unauthorized disclosure of Personal Data and/or (ii) any confirmed unauthorized copying, modification or disposal of Personal Data.

2.12. "Processing" (or alternative variations of the word, such as "Process" or "Processes" as verbs) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.13. "Processor" means the entity which Processes Personal Data on behalf of the Controller.

2.14. "Services" has the meaning set forth in the Service Agreement.

2.15. "Standard Contractual Clauses" or "SCCs" mean the standard data protection clauses adopted by the European Commission for personal data transfer between controllers or processors in the EEA and controllers or processors outside the EEA. Standard contractual clauses adopted by the European Commission are a transfer tool under the GDPR, as per Article 46(2)(c) and (5) of GDPR.

2.16. "Sub-Processor" means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

2.17. "Supervisory Authority" means an independent public authority which is established by a government agency pursuant to a Data Protection Law for the purposes of supervising, auditing and/or enforcing the protections to Personal Data provided by the applicable Data Protection Law.

2.18. "UK Standard Contractual Clauses" means International Data Transfer Addendum to the European Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office under S119A(1) Data Protection Act 2018.

3. **Roles of the Parties.** In the context of the Addendum, the parties agree that:

For the purpose of this Addendum, the parties acknowledge and confirm that Customer is a Controller and Intermedia is a Processor for Processing Personal Data for the Purposes (as defined in Exhibit C to Schedule 1) in the context of the

Intermedia Service, except when Intermedia Processes Personal Data for its own business purposes, such as billing, account management, data analysis, benchmarking, technical support, and product development, in which case Intermedia is a Controller.

4. **Compliance with Data Protection Law**. Each party shall comply with Data Protection Law when Processing Personal Data in the context of the Services.

5. **Obligations of Customer.** Customer confirms and warrants that, in relation to the Processing of Personal Data for the Purposes in the context of the Service, it acts as a Controller and that it:

   5.1. Complies with Data Protection Law when Processing Personal Data, and only gives lawful instructions to Intermedia.

   5.2. Relies on a valid legal ground under Data Protection Law for each Purpose, including obtaining Data Subjects' appropriate consent if required or appropriate under Data Protection Law.

   5.3. Provides appropriate notice to the Data Subjects regarding the Processing of Personal Data for the Purposes, in a timely manner and at the minimum with the elements required under Data Protection Law.

   5.4. Takes reasonable steps to ensure that Personal Data is accurate, complete and current; adequate, relevant and limited to what is necessary in relation to the Purposes for which they are processed; and kept in a form which permits identification of Data Subjects for no longer than is necessary for the Purposes for which the Personal Data are processed unless a longer retention is required or allowed under applicable law.

   5.5. Implements appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with Data Protection Law, including, as appropriate, appointing a data protection officer, maintaining records of processing, complying with the principles of data protection by design and by default and, where required, performing data protection impact assessments and conducting prior consultations with supervisory authorities.

   5.6. Responds to Data Subject requests to exercise their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, (f) objection to the Processing, and (g) not being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, in accordance with Data Protection Law.

   5.7. Cooperates with Intermedia to fulfil their respective data protection compliance obligations in accordance with Data Protection Law.

6. **Obligations of Intermedia.** Intermedia confirms and warrants that in relation to the Processing of Personal Data for the Purposes in the context of the Service, it acts as a Processor, and that it:

   6.1. Only Processes Personal Data on behalf of Customer in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in Exhibit C to Schedule 1 or as otherwise agreed by both parties in writing. For the avoidance of doubt, (a) the parties acknowledge and agree that (i) the reference to "the Customer's lawful written instructions" in the preceding sentence (and elsewhere in this Addendum) includes the Service Agreement and (ii) accordingly, Intermedia's Processing of Personal Data as part of providing the Services shall be deemed to be performed in accordance with the Customer's lawful written instructions; and (b) Customer authorizes Intermedia to de-identify Personal Data for Intermedia's product development, product improvement, benchmarking, marketing and analytics purposes.

   6.2. Will promptly inform Customer if, in its opinion, the Customer's instructions infringe Data Protection Law, or if Intermedia is unable to comply with the Customer's instructions. If Intermedia is unable to comply with the Customer's instructions, Customer is entitled to suspend the communication of Personal Data and/or terminate the Intermedia Service.

   6.3. Will, taking into account the nature of the Processing and the information available to Intermedia, assist Customer in ensuring compliance with Customer's obligations under Data Protection Law, including data security, data breach

notifications, data protection impact assessments, and prior consultations with supervisory authorities. To the extent legally permitted, Customer shall be responsible for any costs arising from Intermedia's provision of such assistance.

6.4. Will, taking into account the nature of the Processing, take appropriate technical and organizational measures to assist Customer in fulfilling Customer's obligation to respond to Data Subjects' requests to exercise their rights as provided under Data Protection Law. In particular, Customer is responsible for requesting assistance from Intermedia and providing Intermedia with all necessary information, including forwarding the Data Subject's request to Intermedia. Any request for assistance must be notified to Intermedia not less than ten (10) days before the time limit for responding to the request in accordance with Data Protection Law. Intermedia is not responsible for responding to or fulfilling any requests received directly from Data Subjects. To the extent legally permitted, Customer shall be responsible for any costs arising from Intermedia's provision of such assistance.

6.5. Will notify the Customer when local laws prevent Intermedia from complying with the instructions received from the Customer via this Addendum, except if such disclosure is prohibited by applicable law on important grounds of public interest, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. Customer is responsible for notifying its competent supervisory authority as applicable and required under Data Protection Law.

6.6. When this Addendum expires or upon termination of this Addendum, Intermedia will, at the choice of Customer, delete or return all the Personal Data to Customer, except that Intermedia shall not be obligated to return or destroy any portion of the Personal Data that: (a) Data Protection Law (i) prevents Intermedia from returning or destroying or (ii) requires Intermedia to store; (b) Intermedia archives in accordance with Intermedia's record retention policies or applicable legal or regulatory requirements; (c) may be necessary or advisable in connection with pending or anticipated litigation; or (d) consists of internal system, activity, network or other similar log data that is reasonably necessary, either by law or in accordance with Intermedia's standard business practices, for Intermedia to retain or store. In the case of any Personal Data retained by Intermedia in accordance with the preceding sentence, Intermedia will protect the confidentiality of the Personal Data and will not actively Process the Personal Data anymore.

7. **Security of the Processing, Confidentiality, and Personal Data Breach Notification**.

7.1. Intermedia has implemented and maintains a comprehensive written information security program that complies with Data Protection Law and Exhibit E to Schedule 1 of this Addendum, including appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes at the minimum the security measures listed in Exhibit E to Schedule 1 hereof and as appropriate: (a) the pseudonymization (or anonymization) or encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) 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 (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing. In assessing the appropriate level of security, Intermedia must take 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 Data Subjects and the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7.2. Intermedia's information security program shall, among other things, include regular testing or otherwise monitoring of the effectiveness of Intermedia's information safeguards as described in Exhibit E. Intermedia must take steps to ensure that any person acting under its authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation.

7.3. Intermedia will inform Customer without undue delay after having become aware of a Personal Data Breach. Intermedia will be considered to be aware of a Personal Data Breach when it has established that a Data Breach has occurred. Intermedia will take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach.

8. **International Data Transfers**.

8.1. To provide the Services, Intermedia may need to import Personal Data to countries other than the country in which the data were originally collected, including without limitation, to the United States. Customer authorizes such cross-border Personal Data transfers and confirms and warrants that it will comply with any requirements under Data Protection Law with regard to such Personal Data transfers.

8.2. Where Intermedia Processes Personal Data from the EEA on behalf of Customer, such International Data Transfers shall be made pursuant to Schedule 1 to this Addendum.

9. **Intermedia's Sub-Processing**. Customer gives a general authorization to Intermedia to disclose Personal Data to Sub-Processors in the context of the Service under the conditions set forth below and Intermedia represents and warrants that:

9.1. When sub-processing the Processing of Personal Data in the context of the Service, Intermedia binds its Sub-Processors by way of an agreement which imposes on the Sub-Processor the same or substantially similar data protection obligations as are imposed on Intermedia under this Addendum, in particular providing sufficient guarantees to implement appropriate technical and organizational measures to ensure the Processing will meet requirements under Data Protection Law, to the extent applicable to the nature of the service provided by the Sub-Processors. Where the Sub-Processor fails to fulfill its data protection obligations under such agreement, Intermedia shall remain fully liable towards Customer for the performance of the Sub-Processor's obligations under such agreement.

9.2. Intermedia agrees to provide Customer with a list of Intermedia's current Sub-Processors and shall notify Customer of any intended addition or replacement of Sub-Processors; provided that Customer must subscribe to receive email notification(s) in such manner as shall be made available by Intermedia through Customer's administrative control panel for Intermedia services. Intermedia shall allow Customer to reasonably object to such changes by notifying Intermedia in writing within ten (10) business days after receipt of Intermedia's notice of the addition or replacement of a Sub-Processor. Customer's objection should be sent to privacy@intermedia.com and explain the reasonable grounds for the objection. If Customer does not object within such period, Customer shall be deemed to have consented to the Processing of Customer's Personal Data by such Sub-Processor. If Customer objects to the addition of a Sub-Processor and Intermedia cannot reasonably accommodate Customer's objection, Intermedia will notify Customer. Upon receipt of Intermedia's notification, Customer may terminate those applicable Services which cannot be provided by Intermedia without the use of such Sub-Processor by providing thirty (30) days written notice to Intermedia.

10. **Data Protection and Security Audit.**

10.1. Upon prior written request by Customer, Intermedia agrees to provide Customer within reasonable time with: (a) a summary of a recent audit report demonstrating Intermedia's compliance with its obligations under this Addendum, after redacting any confidential and/or commercially sensitive information; and (b) confirmation that the audit has not revealed any material vulnerability in Intermedia's systems, or to the extent that any such vulnerability was detected, that Intermedia has appropriately remedied such vulnerability. If the above measures are not reasonably sufficient to confirm compliance with the provisions of Data Protection Law relevant to the Services and their use by Customer, or if they reveal material compliance or security vulnerability issues, then, subject to the strictest confidentiality obligations, Intermedia allows Customer to request an audit of Intermedia's data protection compliance program by an external independent auditor, which shall be jointly selected by the parties. The external independent auditor cannot be a competitor of Intermedia, and the parties will mutually agree upon the scope, timing, and duration of the audit. Intermedia will make available to Customer the result of the audit of its data protection compliance program; provided that Intermedia will have the right to redact any confidential and/or commercially sensitive information from such audit report provided to Customer. Customer shall reimburse Intermedia for all expenses and costs for such audit.

11. **Liability Towards Data Subject.** The parties agree that they will be held liable for violations of Data Protection Law towards Data Subjects as follows:

11.1. Customer is responsible for the damage caused by the Processing which infringes Data Protection Law or this Addendum.

11.2. When Intermedia acts as a Processor, it will be liable for the damage caused by the Processing only where it has not complied with obligations of Data Protection Law specifically directed to Processors or where it has acted outside of or contrary to

Customer's lawful instructions. In that context, Intermedia will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

11.3. Where the parties are involved in the same Processing and where they are responsible for any damage caused by the Processing, both Customer and Intermedia may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If Intermedia paid full compensation for the damage suffered, it is entitled to claim back from Customer that part of the compensation corresponding to Customer's part of responsibility for the damage.

12. **Applicable Law and Jurisdiction**. This Addendum is governed by the law of Ireland; provided that, if Data Protection Law requires that the law of another jurisdiction govern the Processing of any particular Personal Data under this Addendum, the Processing of such Personal Data under this Addendum shall be governed by the law required by Data Protection Law. Any disputes between the parties relating to the Processing of Personal Data under this Addendum will be subject to the exclusive jurisdiction of the courts of Ireland.

13. **List of Schedules**. The schedules hereto form a part of this Addendum and have been attached hereto as follows:

13.1. Schedule 1: EEA Region Specific Terms

13.2. Schedule 2: CCPA Specific Terms

13.3. Schedule 3: United Kingdom Specific Terms

14. **Modification of this Agreement**. This Addendum may only be modified by a written amendment signed by each of the parties, except for any amendment designed to comply with any Data Protection Law or applicable industry standards, which amendment may be made unilaterally by Intermedia.

15. **Termination.** The parties agree that this Addendum is terminated upon the termination of the Services.

16. **Invalidity and Severability.** If any provision of this Addendum is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this Addendum and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

SCHEDULE 1
EEA Region Specific Terms

1. **GDPR**. Intermedia will Process Personal Data in accordance with the GDPR requirements applicable to Intermedia's provision of its Services.

2. **EEA External Data Transfers**. For purposes of this Schedule 1, the term "EEA External Data Transfers" shall mean any transfer of Personal Data from the EEA to an international organization or to a country outside of the EEA and includes any onward transfer of Personal Data from the international organization or the country outside of the EEA to another international organization or to another country outside of the EEA.

    a. Customer hereby authorizes Intermedia to perform EEA External Data Transfers to countries subject to a current adequacy decision of the European Commission or based on Standard Contractual Clauses.

    b. All authorizations of EEA External Data Transfers pursuant to Section 2(a) are expressly conditioned upon each party's ongoing compliance with the requirements of Data Protection Law applicable to EEA External Data Transfers, and any applicable legal instrument for EEA External Data Transfers.

    c. As described by the roles of the parties in Section 3 of the Addendum, Intermedia and Customer agree to Module 1 (Controller-to-Controller) and Module 2 (Controller-to-Processor)(collectively, "Modules") of the Standard Contractual Clauses, which are linked in Exhibit A to this Schedule 1 and are hereby incorporated into this Addendum and form an integral part hereof:

        i. The "data exporter" is Customer and the "data importer" is Intermedia;
        ii. For the Use of Sub-Processor in Clause 9(a) of the Modules, the parties agree to Option 2 and include a specified time period for thirty (30) days;
        iii. For Redress in Clause 11 of the Modules, the optional paragraph has been, and is hereby, struck;
        iv. For Supervision in Clause 13(a) of the Modules, the parties agree to Paragraph 1;
        v. For Governing Law in Clause 17 of the Modules, the parties agree to Option 1 and specify the Ireland as the law governing this Schedule 1;
        vi. For Choice of Forum and Jurisdiction in Clause 18(b) of the Modules, the parties agree to the courts of Ireland as the jurisdiction governing this Schedule 1; and
        vii. Annex I, II and III to the Modules of the Standard Contractual Clauses are Exhibits B through F to this Schedule 1.

    d. The Standard Contractual Clauses will remain in force unless repealed or replaced by the appropriate governing entity, or Intermedia relies on an alternative data transfer mechanism that is recognized under the EEA's Data Protection Law as adducing adequate safeguards for the transfers of Personal Data outside of the EEA. Such alternative data transfer mechanisms include, but are not limited to, Binding Corporate Rules or a new data transfer agreement between the EU and the U.S. In any such event, the parties agree that any such changes shall be made in accordance with Section 14 of the Addendum. In the alternative, if Data Protection Law is deemed to require Customer's signature to amend the Addendum (thus restricting Intermedia's right to amend the Addendum set forth in the preceding sentence), then Customer hereby agrees and commits to execute an amendment to the Addendum, in the form provided by Intermedia, that reflects and incorporates the alternative data transfer mechanism selected by Intermedia.

    e. In case of conflict or inconsistency between the Standard Contractual Clauses and any other current or future agreement between the parties, the Standard Contractual Clauses will prevail. Notwithstanding the foregoing, this provision shall not apply to any additional qualifications, conditions, clarifications, or processes referenced in the Service Agreement or Addendum that supplement the terms of the Standard Contractual Clauses.

Schedule 1
Exhibit A

STANDARD CONTRACTUAL CLAUSES

The Standard Contractual Clauses, as presented in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, are hereby incorporated herein by reference and Customer and Intermedia agree to Module 1 (Controller-to-Controller) and Module 2 (Controller-to-Processor)(collectively, "Modules") of the SCCs.

Schedule 1
Exhibit B

Annex I (A) LIST OF PARTIES

to the Standard Contractual Clauses

Data Exporter(s):

1. **Name of Company**:

   Address:

   Contact Person's Name:

   Contact Person's Position:

   Contact Person's Phone Number:

   Contact Person's Email Address:

   Activities Relevant to the Data Transferred Under These Clauses: See Annex I(B)

   Signature:

   Date:

2. **Role:** Customer acts as Controller for the Processing of Personal Data for the Purposes (as defined in Annex II) in the context of the Intermedia Service.

Data Importer(s):

1. **Name**: Intermedia.net, Inc.

   Address: 100 Mathilda Place, Suite 100, Sunnyvale, California 94086

   Contact Person's Name: Jeffrey Eisenberg

   Contact Person's Position: Chief Administrative Officer and General Counsel

   Contact Person's Email Address: privacy@intermedia.com

   Activities Relevant to the Data Transferred Under These Clauses: See Annex I(B)

   Signature:

   Date:

2. **Role:** Intermedia is a Processor acting on behalf of Customer, for the Processing of Personal Data for the Purposes (as defined in Annex I(B)) in the context of the Intermedia Service, or a Controller when Intermedia Processes Personal Data for its own business purposes, such as billing, account management, data analysis, benchmarking, technical support, and product development.

Schedule 1
Exhibit C

Annex I (B) DESCRIPTION OF TRANSFER
to the Standard Contractual Clauses

Categories of Data Subjects Whose Personal Data is Transferred

Intermedia may Process Personal Metadata (as defined below) relating to any users, senders or recipients of communications or files through the Services, as well as Account-Level User Information (as defined below) relating to any users of Intermedia's services. In addition, Intermedia may Process Personal Data regarding any data subjects regarding whom Customers and end users transmit, receive, store, encrypt and/or copy Personal Data in their use of Intermedia's services.

Categories of Personal Data Transferred

Intermedia may Process any Personal Data that Customers and end users transmit, receive, store, encrypt and/or copy in their use of Intermedia's services. In addition, Intermedia may Process any Personal Data that is included as metadata (such as user names, email addresses, IP addresses and the like) in any communications or files that Intermedia Processes in its delivery of the Services ("**Personal Metadata**"), as well as any Personal Data that is included in Intermedia's account-level business records, such as billing information and history, user account identifiers, access logs and other business operation information ("**Account-Level User Information**").

The Frequency of the Transfer (e.g. whether the data is transferred on a one-off or continuous basis)

The Personal Data is transferred on a continuous basis.

Nature of the Processing

Intermedia will Process Personal Data for the purpose of providing the Services and any associated tools and services, including technical support or other support services.

Purpose(s) of the Data Transfer and Further Processing

Intermedia will Process Personal Data for the purpose of:

- providing the Services and any associated tools and services
- providing support and troubleshooting (preventing, detecting and repairing problems);
- ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, and security); and
- activities contemplated to be conducted by Intermedia under Intermedia's Privacy Policy

The Period for Which the Personal Data Will be Retained, or, If That is Not Possible, the Criteria Used to Determine that Period

Intermedia will Process Personal Data for as long as reasonably necessary in connection with the operation of its business and as permitted under the Service Agreement and this Addendum.

For Transfers to (Sub-)Processors, also Specify Subject Matter, Nature and Duration of the Processing

Sub-processors shall Process Personal Data only as necessary, and for as long as necessary, to provide the Services in accordance with the applicable agreement with Intermedia.

Schedule 1
Exhibit D

Annex I (C) COMPETENT SUPERVISORY AUTHORITY
to the Standard Contractual Clauses

Identify the Competent Supervisory Authority/ies in Accordance with Clause 13

Dutch Data Protection Supervisory Authority (Autoriteit Persoonsgegevens) or such other supervisory authority as may be required under applicable law.

Schedule 1
Exhibit E

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA
to the Standard Contractual Clauses

This Annex forms part of the Clauses, and, by signing the Addendum, the parties agree to the terms referenced herein.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clause 8 (or document/legislation attached):

Intermedia will implement the following types of security measures:

1. Physical access control

Technical and organizational measures designed to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are Processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff;
- Surveillance facilities, video/CCTV monitor, alarm system; and
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures designed to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g., password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts; and
- Encryption of archived data media.

3. Data access control

Technical and organizational measures designed to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;

- Encryption; and
- Pseudonymisation.

4. Disclosure control

Technical and organizational measures designed to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/tunneling;
- Logging; and
- Transport security.

5. Entry control

Technical and organizational measures designed to monitor whether Personal Data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems; and
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures designed to ensure that Personal Data are Processed solely in accordance with the instructions of the Controller include:

- The terms of, and performance by Intermedia of its obligations under, the Service Agreement;
- Formal commissioning (request form); and
- Criteria for selecting the Processor.

7. Availability control

Technical and organizational measures designed to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan; and
- Business Continuity Plan.

8. Separation control

Technical and organizational measures designed to ensure that Personal Data collected for different purposes can be Processed separately include:

- Separation of databases;
- "Internal client" concept / limitation of use; and
- Segregation of functions (production/testing).

9. Management control

Technical and organizational measures designed to ensure that Personal Data accessed, processed, and/or stored are monitored and managed in line with industry standards, including the security controls and assurance activities under SSAE18 (SOC 2 Type 2), ISO 27001 or similar certification or audits:

- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing;
- Regular application and network security testing;
- Internal IT and IT security governance and management;
- Measures for ensuring system configuration; and
- Measures for certification/assurance of processes and products.

10. Data Management control

Technical and organizational measures designed to ensure that Personal Data accessed, processed, and/or stored are monitored and managed pursuant to the Data Protection Law and include:

- Measures for ensuring data minimization;
- Measures for ensuring data quality;
- Measures for ensuring limited data retention; and
- Measures for allowing data portability and ensuring erasure.

For transfers to (Sub-) Processors, also describe the specific technical and organisational measures to be taken by the (Sub-) Processor to be able to provide assistance to the Controller and, for transfers from a Processor to a Sub-Processor, to the Data Exporter.

The specific technical and organizational measures by each Sub-Processor shall be substantially similar to the security measures set forth herein as agreed upon between Intermedia and the applicable Sub-Processor(s).

Schedule 1
Exhibit F

ANNEX III – LIST OF SUB-PROCESSORS
to the Standard Contractual Clauses

Customer has authorised the use of the Sub-Processors listed in the Sub-Processor List provided by Intermedia.

SCHEDULE 2
CCPA Specific Terms

1. **Definitions**. For the purposes of this Schedule 2:

   1.1. The capitalized terms used in this Schedule 2 and not otherwise defined in this Schedule 2 shall have the definitions set forth under the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 to 1798.199) and its implementing regulations, as amended or superseded from time to time ("**CCPA**").

2. **Roles and Scope.**

   2.1. In furtherance of obligations under the CCPA, this Schedule 2 applies only to the Collection, retention, use, disclosure, and Sale of Personal Information provided by Customer to, or which is Collected on behalf of Customer by, Intermedia to provide Services to Customer pursuant to the Addendum or to perform a Business Purpose ("**Intermedia Personal Information**").

   2.2. The parties acknowledge and agree that Customer is a Business and appoints Intermedia to process Customer Personal Information on behalf of Customer.

3. **Restrictions on Processing.**

   3.1. Except as otherwise permitted by the CCPA, Intermedia is prohibited from (i) retaining, using, or disclosing Customer Personal Information for any purpose other than for the specific purpose of performing the Services specified in the Addendum for Customer, as set out in this Schedule 2 and (ii) further Collecting, Selling, or using Intermedia Personal Information except as necessary to perform the Services.

4. **Consumer Rights.**

   4.1. Intermedia shall provide commercially reasonable assistance to Customer for the fulfillment of Customer's obligations to respond to CCPA-related Customer rights requests regarding Customer Personal Information.

5. **Notice.**

   5.1. Customer represents and warrants that it has provided notice that Customer Personal Information is being used or shared consistent with Cal. Civ. Code 1798.140(t)(2)(C)(i).

6. **CCPA Exemption.**

   6.1. Notwithstanding any provision to the contrary of the Service Agreement or this Addendum, the terms of this Addendum shall not apply to Intermedia's processing of Customer Personal Information that is exempt from the CCPA, including under Cal. Civ. Code 1798.145(a).

SCHEDULE 3
United Kingdom Specific Terms

1. Intermedia will Process Personal Data in accordance with the applicable Data Protection Law of the United Kingdom ("UK"), including UK General Data Protection Regulation ("UK GDPR") and Data Protection Act 2018 (collectively, "UK Data Protection Law"), for Intermedia's provision of its Services in the UK.

2. **UK External Data Transfers**. For purposes of this Schedule 3, the term "UK External Data Transfers" shall mean any transfer of Personal Data from the UK to an international organization or to a country outside of the UK and includes any onward transfer of Personal Data from the international organization or the country outside of the UK to another international organization or to another country outside of the UK.

    a. Customer hereby authorizes Intermedia to perform UK External Data Transfers to countries subject to a current adequacy decision of the UK or based on the UK Standard Contractual Clauses.

    b. All authorizations of UK External Data Transfers pursuant to Section 2(a) are expressly conditioned upon each party's ongoing compliance with the requirements of UK Data Protection Law applicable to UK External Data Transfers, and any applicable legal instrument for UK External Data Transfers.

    c. As described by the roles of the parties in Section 3 of the Addendum, Intermedia and Customer agree to the UK Standard Contractual Clauses, which are hereby incorporated into this Addendum and form an integral part hereof:

        i. As referenced in Part 1 of the UK Standard Contractual Clauses, the following shall apply:
            1. The parties referenced in Table 1 refer to the parties referenced in Exhibit B to Schedule 1 of the Addendum.
            2. Under Table 2, the parties agree to Option 1, effective as of the Effective Date of this Addendum, as referenced in Section 2(c) of Schedule 1 to the Addendum.
            3. Under Table 3, the following shall apply:
                a. "Annex 1A: List of Parties" is Exhibit B to Schedule 1 of this Addendum.
                b. "Annex 1B: Description of Transfer" is Exhibit C to Schedule 1 of this Addendum.
                c. "Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data" is Exhibit E to Schedule 1 of this Addendum.
                d. "Annex III List of Sub processors" is Exhibit F of this Addendum.
            4. Under Table 4, the parties agree that the Importer may end this Schedule 3 pursuant to Section 19 of the UK Standard Contractual Clauses.
        ii. As referenced in Part 2 of the UK Standard Contractual Clauses, the parties agree to the Mandatory Clauses.

d. The UK Standard Contractual Clauses will remain in force unless repealed or replaced by the appropriate governing entity, or Intermedia relies on an alternative data transfer mechanism that is recognized under the UK's Data Protection Law as adducing adequate safeguards for the transfers of Personal Data outside of the UK. Such alternative data transfer mechanisms include, but are not limited to, Binding Corporate Rules or a new data transfer agreement between the UK and the U.S. In any such event, the parties agree that any such changes shall be made in accordance with Section 14 of the Addendum. In the alternative, if UK Data Protection Law is deemed to require Customer's signature to amend the Addendum (thus restricting Intermedia's right to amend the Addendum set forth in the preceding sentence), then Customer hereby agrees and commits to execute an amendment to the Addendum, in the form provided by Intermedia, that reflects and incorporates the alternative data transfer mechanism selected by Intermedia.

e. In case of conflict or inconsistency between the UK Standard Contractual Clauses and any other current or future agreement between the parties, the UK Standard Contractual Clauses will prevail for UK External Data Transfers. Notwithstanding the foregoing, this provision shall not apply to any additional qualifications, conditions, clarifications, or processes referenced in the Service Agreement or Addendum that supplement the terms of the UK Standard Contractual Clauses.