CUSTOMER GDPR DATA PROCESSING ADDENDUM FOR ISPS (HOMEPASS)

This Data Processing Addendum ("**DPA**") amends and forms part of the Managed WiFi Services Agreement (the "**Agreement**") between Plume Design, Inc. ("**Plume**") and [Provider's full name] ("**Provider**"). This DPA prevails over any conflicting term of the Agreement, but does not otherwise modify the Agreement.

1. Definitions

1.1. In this DPA:

a) "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory Authority**" have the meaning given to them in the GDPR;

b) "**Data Protection Law**" means General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), and their national implementations in the European Economic Area ("**EEA**"), Switzerland and the United Kingdom, each as applicable, and as may be amended or replaced from time to time;

c) "**Data Subject Rights**" means Data Subjects' rights to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making in accordance with Data Protection Law;

d) "**International Data Transfer**" means any transfer of Provider Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom;

e) "**Provider Personal Data**" means any Personal Data, the Processing of which is subject to Data Protection Law, for which Provider or Provider's customer is the Controller, and which is Processed by Plume to provide the Services;

f) "**Subprocessor**" means a Processor engaged by Plume to Process Provider Personal Data; and

g) "**Standard Contractual Clauses**" means the clauses annexed to EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5-18), as may be amended or replaced from time to time.

1.2. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

2. Scope and applicability

2.1. This DPA applies to Processing of Provider Personal Data by Plume to provide the Services.

2.2. The subject matter, nature and purpose of the Processing, the types of Provider Personal Data and categories of Data Subjects are set out in the Agreement and in **Appendix 1**.

2.3. Provider is a Controller and appoints Plume as a Processor on behalf of Provider. Provider is responsible for compliance with the requirements of Data Protection Law applicable to Controllers.

2.4. If Provider is a Processor on behalf of other Controller(s), then Provider: is the single point of contact for Plume; must obtain all necessary authorizations from such other Controller(s); undertakes to issue all instructions and exercise all rights on behalf of such other Controller(s); and is responsible for compliance with the requirements of Data Protection Law applicable to Processors.

2.5. Provider acknowledges that Plume may Process Personal Data relating to the operation, support, or use of the Services for its own business purposes, such as billing, account management, data analysis, benchmarking, technical support, product and service improvement and development, and compliance with law. Plume is the Controller for such Processing, will Process such data in accordance with Data Protection Law; and is solely responsible for the lawfulness of such Processing.

2.6. Provider shall provide Data Subjects with a link to the Plume Privacy Policy available on Plume's website and notify Data Subjects that the Plume Privacy Policy describes how their Personal Data will be Processed by Plume for its own business purposes.

3. **Instructions**

3.1. Plume will Process Provider Personal Data to provide the Services and in accordance with Provider's documented instructions.

3.2. The Controller's instructions are documented in this DPA, the Agreement, and any applicable statement of work.

3.3. Provider may reasonably issue additional instructions as necessary to comply with Data Protection Law. Plume may charge a reasonable fee to comply with any additional instructions.

3.4. Unless prohibited by applicable law, Plume will inform Provider if Plume is subject to a legal obligation that requires Plume to Process Provider Personal Data in contravention of Provider's documented instructions.

4. **Personnel**

4.1. Plume will ensure that all personnel authorized to Process Provider Personal Data are subject to an obligation of confidentiality.

5. **Security and Personal Data Breaches**

5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Plume will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures listed in **Appendix 2**.

5.2. Provider acknowledges that the security measures in **Appendix 2** are appropriate in relation to the risks associated with Provider's intended Processing, and will notify Plume prior to any intended Processing for which Plume's security measures may not be appropriate.

5.3. Plume will notify Provider without undue delay after becoming aware of a Personal Data Breach involving Provider Personal Data. If Plume's notification is delayed, it will be accompanied by reasons for the delay.

6. **Subprocessing**

6.1. Provider hereby authorizes Plume to engage Subprocessors. A list of Plume's current Subprocessors is included in **Appendix 0**.

6.2. Plume will enter into a written agreement with Subprocessors which imposes the same obligations as required by Data Protection Law.

6.3. Plume will notify Provider prior to any intended change to Subprocessors. Plume may do so (i) by notifying the Provider in writing, or (ii) by making available a Plume managed URL, provided that Plume shall inform Provider of such URL. Provider may object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following Plume's notification of the intended change. Provider and Plume will work together in good faith to address Provider's objection. If Plume chooses to retain the Subprocessor, Plume will inform Provider at least thirty (30) days before authorizing the Subprocessor to Process Provider Personal Data, and in case of a security threat, Provider may immediately discontinue using the relevant parts of the Services, and may terminate the relevant parts of the Services within thirty (30) days.

7. **Assistance**

7.1. Taking into account the nature of the Processing, and the information available to Plume, Plume will assist Provider, including, as appropriate, by implementing technical and organizational measures, with the fulfilment of Provider's own obligations under Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct data protection impact assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.

7.2. Plume will maintain records of Processing of Provider Personal Data in accordance with Data Protection Law.

7.3. Plume may charge a reasonable fee for assistance under this **Section 7**. If Plume is at fault, Plume and Provider shall each bear their own costs related to assistance.

8. Audit

8.1. Plume must make available to Provider all information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by a Supervisory Authority or reasonably requested by Provider and performed by an independent auditor as agreed upon by Provider and Plume. Unless mandated by a Supervisory Authority, Provider may not request the performance of an audit, including an inspection, more than once per year and must notify Plume forty-five (45) days prior to any such audit or inspection.

8.2. Plume will inform Provider if Plume believes that Provider's instruction under **Section 8.1** infringes Data Protection Law. Plume may suspend the audit or inspection, or withhold requested information until Plume has modified or confirmed the lawfulness of the instructions in writing.

8.3. Provider bears all costs related to audits, including inspections.

9. International Data Transfers

9.1. Provider hereby authorizes Plume to perform International Data Transfers on the basis of an adequacy decision by the EU Commission, on the basis of Standard Contractual Clauses, or otherwise in accordance with Data Protection Law. .

9.2. By signing this DPA, Provider and Plume conclude the Standard Contractual Clauses, which are hereby incorporated into this DPA and completed as follows: the "data exporter" is Provider; the "data importer" is Plume; the governing law in Clause 9 and Clause 11.3 of the Standard Contractual Clauses is the law of the country where Provider is established; Appendix 1 and 2 to the Standard Contractual Clauses are Appendix 1 and 2 to this DPA, respectively; and the optional indemnification clause is struck. Where Personal Data is transferred outside of the United Kingdom based on the Standard Contractual Clauses, the following changes apply: (i) references to Data Protection Law are replaced with references to applicable UK data protection law, (ii) references to the EU or Member States are replaced with references to the United Kingdom, (iii) references to EU authorities are replaced with references to the competent UK authority, and (iv) references to the Member State governing law in Clause 9 and Clause 11.3 of the Standard Contractual Clauses are replaced with references to the law of England and Wales.

9.3. If Plume's compliance with Data Protection Law applicable to International Data Transfers is affected by circumstances outside of Plume's control, including if a legal instrument for International Data Transfers is invalidated, amended, or replaced, then Provider and Plume will work together in good faith to reasonably resolve such non-compliance.

10. Notifications

10.1. Provider will send all notifications, requests and instructions under this DPA to Plume's Information Security and Legal Department via email to legal@plume.com.

11. Liability

11.1. To the extent permitted by applicable law, where Plume has paid damages or fines, Plume is entitled to claim back from Provider that part of the compensation, damages or fines, corresponding to Provider's part of responsibility for the damages or fines.

12. **Termination and return or deletion**

12.1. This DPA is terminated upon the termination of the Agreement.

12.2. Provider may request return of Provider Personal Data up to ninety (90) days after termination of the Agreement. Unless required or permitted by applicable law, Plume will delete all remaining copies of Provider Personal Data within one hundred eighty (180) days after returning Provider Personal Data to Provider.

13. **Modification of this DPA**

13.1. This DPA may only be modified by a written amendment signed by both Plume and Provider.

14. **Invalidity and severability**

14.1. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

Plume	**Provider:**
Name: Vincent Samuel	Name:
Title: Head of Data Protection	Title:
Address: 290 California Ave #200, Palo Alto, CA 94306	Address:
Signature: Vincent Samuel	Signature:
Date: April 25th 2021	Date:

APPENDIX 0

SUBPROCESSORS

#	Name
1.	AWS, Amazon.com, Inc. – Cloud software services
2.	Plume Design d o.o. Ljubljana, Slovenia – Research and development services from Plume's Slovenia, Poland, Switzerland offices
3.	Majorel Canada, Inc. – Customer support services
4.	Zendesk, Inc. – Customer support services
5.	Sykes Enterprises, Inc. – Customer support services
6.	Cognitive Systems Corp - Technology vendor for Plume Motion

APPENDIX 1

DESCRIPTION OF THE PROCESSING - HOMEPASS

1. Data Subjects

The Provider Personal Data Processed concern the following categories of Data Subjects (please specify):

#	Category
1.	End users

2. Categories of Provider Personal Data

The Provider Personal Data Processed concern the following categories of data (please specify):

#	Category
1.	User account ● First Name, last name, alternatively: system generated name ● Clear name or system generated name (in most partner integrations Plume may not have access to the real end users' names; in such cases the system uses a field for a system generated unique "name" based on the account ID) ● (Login) email address ● Account ID ● Customer ID ● Email address, email ID ● Partner ID ● Password
2.	Location ● Region (US, UK, EU, SG, JP, etc.) ● Name, Created time, onboarded time ● GeoIP, WAN IP, latitude, longitude ● City, state, ZIP/ postal code, country ● Timezone ● ISP
3.	Network Configuration ● ISP ● Network status (online/ offline/ partial), time since. Indicates the networking addresses of the devices and system used to communicate with Plume and the internet along with the operating statistics of the Wi-Fi and internet connections. ● WiFi settings ● WiFi SSID, key ● WiFi encryption, encryption mode ● Primary/ secondary DNS ● DHCP Reservations, port forwarding. Static IP assignments to client devices, port forwarding rules from router to client devices.

4.	HomePass: ● Access zones ● Passwords ● Policies ● Location ID ● Wifi SSID ● PSK ● PSK zone ● PSK assignment ● PSK status ● PSK expiry
5.	Profiles: ● Profile ID ● Name of person in profile ● Primary Device of person in profile ● Assigned Devices of person in profile ● Profile image ● Last Home
6.	Parental Controls: ● Device freeze policies
7.	Nodes (CPE Access Points): ● Nickname ● Model ● ID, location and customer the node is claimed to ● Serial number ● MAC address of nodes ● Performance Data ● Node connected time ● Firmware version
8.	Device ● Device MAC ● Device Nickname ● Type of device (category, brand, name, value, model, device type ID), icon, operating system name and version ● Device typing features (dynamic host configuration protocol (“DHCP”) options, vendor class ID, HTTP user agents, UPnP, mDNS discovery information, DNS FQDNs)

	● Attributes gleaned from network metadata including (but not limited to) its DHCP fingerprint, a sampling of domain name system (“DNS”) requests, device hostname, the nickname given to the device and the unique addresses of the device. ● Performance data.
9.	Network Activity ● Data consumption of the end user devices and CPE nodes (transmitted/ received bytes). ● Client Steering History - (including, but not limited to WAN IP, MAC Address, Hostname, Nickname) ● Network topology data. This information depicts the connections between client devices in use and the Plume network access points serving Wi-Fi. Includes radios/ channels and connection state
10.	Service statistics and Logs Speed Test ● Speed Test Results - ISP, ISP speeds, Outages, Upload & Download speeds history over time App Usage Analytics ● Plume Mobile App (iOS / Android) usage stats (Features used / Screen views) ● Customer ID, ● Location ID, ● First Name, ● Last Name, ● Email, ● City, ● State, ● Country, ● Region, ● Carrier, ● IFA, ● App Version, ● OS / version, ● Manufacturer, ● Device model, ● Time zone, ● Last Used. Logs ● Log information such as messages from the Plume pods regarding Plume connected devices, device inventory data, and software and hardware versions. ● Server Logs from all Plume Services
11.	Plume AI Security: ● DNS queries

	● Blocked DNS queries - Websites (FQDN) blocked for Online protection, IoT protection, Content Filtering for a location or person profile or device ● Source & Destination traffic headers - IP Flows (Source, Destination IP & Port, Protocol, Packets & Byte counts) & App Time Online detected from IP Flows
12.	Plume Motion (information regarding disruptions in WiFi waves in the periphery of Plume network access points and devices connected to the Plume network): ● Configuration of Sounding Devices ● Live motion per location ● Motion Density history (entire network) ● Home Security Events ● State History
13.	Digital Wellbeing ● Source & Destination traffic headers - IP Flows (Source, Destination IP & Port, Protocol, Packets & Byte counts) & App Time Online detected from IP Flows
14.	Crash Reports ● Crash reports. Plume collects crash reports for both the Plume Software and the Plume App. These reports can include information such as the type of crash, the software version that is running and the operating system version of the device running the Plume App.

3. **Sensitive data**

The Provider Personal Data Processed concern the following special categories of data (please specify):

#	Category
1.	The Services are not intended to Process special categories of data.

4. **Processing operations**

The Provider Personal Data will be subject to the following basic Processing activities (please specify):

#	Operation
1.	Data is shared between the parties for Plume to be able to compute, store and continuously refine algorithms used to provide the Services.
2.	To operate and provide users with the Plume Services and tailor them to the users as instructed by the Provider and to fulfill Plume's contractual obligations. This may include ● creating an user account, ● verifying users' identities, ● communicating with users via the Plume App, ● providing customer support, ● arranging the delivery or other provision of products and services or their updates, ● identifying users' devices, e.g. to more accurately represent these devices in the Plume App, ● providing more accurate security threat identification, ● providing better visibility into the user's distributed network,

	● providing reports that help to better understand network bandwidth and the devices that are consuming network resources, ● scheduling network optimizations, firmware updates and internet freeze for user’s devices, ● presenting live motion visuals and motion history, ● providing visibility and control over time spent by users on various Internet applications (app time usage detection), ● alerting the user of malicious Internet locations or websites and content that has been identified as inappropriate in accordance with the content filters set by the Plume App user, ● preventing home devices from being hacked, ● app reporting and analytics, ● identifying device behavior that may indicate an anomaly or attack, ● detecting, preventing, or otherwise addressing fraud, security, or technical issues related to the Plume Services or those of the Provider, including troubleshooting.
3.	To comply with applicable laws regarding the processing of Personal Data on behalf of the Provider as described above and governed by this DPA.
4.	To protect the safety, integrity, rights, or security of the users, the Plume Services or equipment, or any third party.
5.	To ensure compliance with the regulatory requirements for the specific region.

APPENDIX 2

SECURITY MEASURES

Plume will implement the following types of security measures:

1. **Physical access control**

Technical and organizational measures 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 Provider 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, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system; and
- Securing decentralized data processing equipment and personal computers.

5. **Virtual access control**

Technical and organizational measures 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
- Creation of *one* master record per user, user-master data procedures per data processing environment.

6. **Data access control**

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Provider Personal Data in accordance with their access rights, and that Provider 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 Provider Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure; and
- Encryption.

7. **Disclosure control**

Technical and organizational measures to ensure that Provider 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 Provider Personal Data are disclosed, include:

- Logging; and
- Transport security.

8. **Entry control**

Technical and organizational measures to monitor whether Provider 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.

9. **Control of instructions**

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

- Unambiguous wording of the contract;
- Formal commissioning (request form); and
- Criteria for selecting the Processor.

10. **Availability control**

Technical and organizational measures to ensure that Provider 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; and
- Disaster recovery plan.

11. **Separation control**

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

- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing); and
- Procedures for storage, amendment, deletion, transmission of data for different purposes.