Plume

CUSTOMER GDPR DATA PROCESSING ADDENDUM FOR SMALL BUSINESSES (WORKPASS)

This Data Processing Addendum ("**DPA**") amends and forms part of the Plume WorkPass Membership and Cloud Services Agreement (the "**Agreement**") between Plume Design, Inc. ("**Plume**") and [Small Business Customer] ("**Customer**"), which involves the provision of the services described in the Agreement (the "**Services**"). This DPA prevails over any conflicting term of the Agreement, but does not otherwise modify it.

1. **Definitions**
   1.1. "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory Authority**" have the meaning given to them in the GDPR;
   1.2. "**Data Protection Law**" means General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), 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;
   1.3. "**Customer Personal Data**" means any Personal Data, the Processing of which is subject to Data Protection Law, for which Customer is the Controller, and which is Processed by Plume to provide the Services;
   1.4. "**International Data Transfer**" means any transfer of Customer 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;
   1.5. "**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.

2. **Roles of the Parties**
   2.1. Customer is a Controller and appoints Plume as a Processor on behalf of Customer. Customer is responsible for compliance with Data Protection Law applicable to Controllers.
   2.2. Customer 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.
   2.3. Customer must provide Data Subjects with a link to the Plume Privacy Policy available at https://www.plume.com/homepass/legal?tabId=privacy and notify Data Subjects that the Plume Privacy Policy describes how their Personal Data will be Processed (i) by Plume on behalf of Customer, and (ii) by Plume for its own business purposes.

3. **Instructions.** Plume will Process Customer Personal Data to provide the Services and in accordance with Customer's instructions, as documented in this DPA, the Agreement, and any applicable statement of work. Unless prohibited by applicable law, Plume will inform Customer if Plume is subject to a legal obligation that requires Plume to Process Customer Personal Data in contravention of Customer's documented instructions.

4. **Personnel.** Plume will ensure that all personnel authorized to Process Customer Personal Data are subject to an obligation of confidentiality.

5. **Security and Personal Data Breaches.** 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. Plume will notify Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data.

6. **Subprocessing.** Customer hereby authorizes Plume to engage subprocessors to process Customer Personal Data. A list of Plume's current subprocessors is included in Appendix 0 available at [www.plume.com].

7. **Assistance.** Taking into account the nature of the Processing, and the information available to Plume, Plume will assist Customer with the fulfilment of Customer's own obligations under Data Protection Law to: comply with requests to exercise data subject rights under the GDPR; conduct data protection impact assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.

8. **Audit.** Plume must make available to Customer 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 Customer and performed by an independent auditor as agreed upon by Customer and Plume. Unless mandated by a Supervisory Authority, Customer 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. Plume will inform Customer if Plume believes that Customer's instruction under this Section 8 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. Customer bears all costs related to audits, including inspections.

9. **International Data Transfers**
   9.1. Customer 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, Customer and Plume conclude the Standard Contractual Clauses, which are incorporated into this DPA and completed as follows: the "data exporter" is Customer; 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 Customer 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.

10. **Notifications.** Customer will send all notifications, requests and instructions under this DPA to Plume via email to legal@plume.com.

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

12. **Termination and return or deletion.** This DPA is terminated upon the termination of the Agreement. Customer may request return of Customer 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 Customer Personal Data within one hundred eighty (180) days after returning Customer Personal Data.

Plume	**Customer:**
Name: Vincent Samuel	Name:
Title: Head of Data Protection	Title:
Address: 290 California Ave #200, Palo Alto, CA	Address:
Signature: Vincent Samuel	Signature:

Date: May 4th 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
7.	Guest Networks Inc. dba MyWiFi Networks, Toronto Canada - Captive Portal

APPENDIX 1

DESCRIPTION OF THE PROCESSING - WORKPASS

1. **Data Subjects**

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

#	Category
1.	End users

2. **Categories of Customer Personal Data**

The Customer 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 systems 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.	Profiles: ● Profile ID ● Name of person in profile ● Primary Device of person in profile ● Assigned Devices of person in profile ● Profile image ● Last Home
5.	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
6.	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.
7.	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
8.	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
9.	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
10.	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 Customer 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 Customer 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 Customer 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, ● 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 Customer, including troubleshooting.
3.	To comply with applicable laws regarding the Processing of Personal Data on behalf of the Customer 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 Customer 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.

2. **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.

3. **Data access control**

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

4. **Disclosure control**

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

- Logging; and
- Transport security.

5. **Entry control**

Technical and organizational measures to monitor whether Customer 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 to ensure that Customer 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.

7. **Availability control**

Technical and organizational measures to ensure that Customer 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.

8. **Separation control**

Technical and organizational measures to ensure that Customer 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.