Plume

VENDOR GDPR DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") amends and forms part of the written agreement between Plume Design, Inc. ("**Plume**") and [Vendor, Inc.] ("**Vendor**") titled [the Agreement] and dated [Complete] (the "**Agreement**"). 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 Data Protection Law;

b) "**Data Protection Law**" means Regulation (EU) 2016/679, Directive 2002/58/EC (as amended by Directive 2009/136/EC), and all other data protection laws of the European Union, the European Economic Area ("**EEA**"), and their respective member states, Switzerland and the United Kingdom, and any legal instrument for International Data Transfers, each as applicable, and as may be amended or replaced from time to time;

c) "**Data Subject Rights**" means all rights granted to Data Subjects by Data Protection Law, including the right to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making;

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

e) "**Personnel**" means any natural person acting under the authority of Vendor;

f) "**Sensitive Data**" means any type of Personal Data that is designated as a sensitive or special category of Personal Data, or otherwise subject to additional restrictions under Data Protection Law or other laws to which the Controller is subject;

g) "**Subprocessor**" means a Processor engaged by a Processor to carry out Processing on behalf of a Controller;

h) "**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), and as may be amended or replaced from time to time; and

i) "**Third-Party Controller**" means a Controller for which Plume is a Processor.

2. **Roles**

2.1. Plume is a Controller and appoints Vendor as a Processor on behalf of Plume.

2.2. To the extent that Plume is a Processor on behalf of a Third-Party Controller, Plume engages Vendor as a Processor to Process Personal Data on behalf of that Third-Party Controller. To the extent necessary for Plume or a Third-Party Controller to comply with Data Protection Law, Plume may assign certain or all rights granted to Plume in this DPA to that Third-Party Controller.

3. **Scope**

3.1. This DPA applies to the Processing of Personal Data by Vendor in the context of the Agreement.

3.2. The subject matter, nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set out in the Agreement and **Appendix 1**, which is an integral part of this DPA.

4. **Instructions**

4.1. Vendor must only Process Personal Data on documented instructions of Plume or a Third-Party Controller, and is prohibited from Processing Personal Data for any other purpose.

4.2. Plume and Third-Party Controller's instructions are documented in the Agreement, **Appendix 1**, and any applicable statement of work.

4.3. Both Plume and Third-Party Controller may issue additional instructions to Vendor as they deem necessary to comply with Data Protection Law.

5. **Subprocessing**

5.1. Vendor must obtain Plume's specific prior written authorization to engage Subprocessors. Plume hereby authorizes Vendor to engage the Subprocessors listed in **Appendix 0**.

5.2. Vendor must inform Plume at least thirty (30) days prior to any intended change of Subprocessor.

5.3. Vendor must obtain sufficient guarantees from all Subprocessors that they will implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Law and this DPA.

5.4. Vendor must enter into a written agreement with all Subprocessors which imposes the same obligations on the Subprocessors as this DPA imposes on Vendor.

5.5. Vendor must provide a copy of Vendor's agreements with Subprocessors to Plume upon request. Vendor may redact commercially sensitive information before providing such agreements to Plume.

5.6. If any Subprocessor fails to fulfil its obligations under Data Protection Law, this DPA, or the agreements between Vendor and Subprocessor, Vendor will be fully liable to Plume for the performance of such obligations.

6. **International Data Transfers**

6.1. Vendor must obtain Plume's specific prior written authorization to perform International Data Transfers. Plume hereby authorizes Vendor to perform International Data Transfers:

a) to any country subject to a valid adequacy decision of the EU Commission;

b) to the extent authorized by Supervisory Authorities on the basis of an organization's binding corporate rules; and

c) to any other data importer on the basis of Standard Contractual Clauses.

6.2. By signing this DPA, Plume and Vendor conclude the Standard Contractual Clauses, which are hereby incorporated into this DPA and completed as follows: the "data exporter" is Plume; the "data importer" is Vendor; the governing law in Clause 9 and Clause 11.3 of the Standard Contractual Clauses is the law of Slovenia; 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.

6.3. Vendor must inform Plume at least thirty (30) days prior to any intended change of International Data Transfers, including the country, and the legal basis of the International Data Transfer pursuant to **Section 6.1**.

6.4. All authorizations of International Data Transfers in **Section 6** are expressly conditioned upon Vendor's ongoing compliance with the requirements of Data Protection Law applicable to International Data Transfers, and any applicable legal instrument for International Data Transfers. If such compliance is affected by circumstances outside of Vendor's control, including circumstances

affecting the validity of an applicable legal instrument, Plume and Vendor will work together in good faith to reasonably resolve such non-compliance.

7. **Personnel**

7.1. Vendor must implement appropriate technical and organizational measures to ensure that Personnel do not Process Personal Data except on the instructions of the Controller.

7.2. Vendor must ensure that all Personnel authorized to Process Personal Data are subject to a contractual or statutory obligation of confidentiality.

7.3. Vendor must regularly train Personnel regarding the protection of Personal Data.

8. **Security and Personal Data Breaches**

8.1. Vendor must implement technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing, including:

a) encryption and pseudonymization of Personal Data;

b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing;

c) measures to detect Personal Data Breaches in a timely manner;

d) measures to restore the availability and access to Personal Data in a timely manner in the event of an incident;

e) processes for regularly testing, assessing and evaluating the effectiveness of the security measures; and

f) as appropriate, and without limiting the foregoing, the measures listed in **Appendix 2**.

8.2. Vendor must inform Plume without undue delay and no later than 48 hours after becoming aware of a Personal Data Breach. Vendor must, either in the initial notice or in subsequent notices as soon as the information becomes available, inform Plume of the nature of the Personal Data Breach, the categories and number of Data Subjects, the categories and amount of Personal Data, the likely consequences of the Personal Data Breach, and the measures taken or proposed to be taken to address the Personal Data Breach and mitigate possible adverse effects. If Vendor's notice or subsequent notices are delayed, they must be accompanied by reasons for the delay.

8.3. Vendor must document all Personal Data Breaches, including at least the information referred to in **Section 8.2**, and provide a copy to Plume upon request.

9. **Assistance**

9.1. Vendor must assist Plume, including by implementing appropriate technical and organizational measures, with the fulfilment of Plume's own obligations under Data Protection Law, including:

a) complying with Data Subjects' requests to exercise Data Subject Rights;

b) replying to inquiries or complaints from Data Subjects;

c) replying to investigations and inquiries from Supervisory Authorities;

d) conducting data protection impact assessments, and prior consultations with Supervisory Authorities; and

e) notifying Personal Data Breaches.

9.2. Unless prohibited by Swiss, United Kingdom, EU, EEA, or their respective member states' law, Vendor must inform Plume without undue delay if Vendor:

a) receives a request, complaint or other inquiry regarding the Processing of Personal Data from a Data Subject or Supervisory Authority;

b) receives a binding or non-binding request to disclose Personal Data from law enforcement, courts or any government body;

c) is subject to a legal obligation that requires Vendor to Process Personal Data in contravention of Plume's instructions; or

d) is otherwise unable to comply with Data Protection Law or this DPA.

9.3. Unless prohibited by Swiss, United Kingdom, EU, EEA, or their respective member states' law, Vendor must obtain Plume's written authorization before responding to, or complying with any requests, orders, or legal obligations referred to in **Section 9.2**.

10. **Accountability**

10.1. Vendor warrants that it possesses the expert knowledge, reliability and resources, and has implemented appropriate technical and organizational measures to meet the requirements of Data Protection Law, including for the security of the Processing.

10.2. Vendor must maintain records of all Processing of Personal Data, including at a minimum the categories of information required under Data Protection Law, and must provide a copy of such records to Plume upon request.

10.3. Vendor must inform Plume without undue delay if Vendor believes that an instruction of Plume violates Data Protection Law, in which case Vendor may suspend the Processing until Plume has modified or confirmed the lawfulness of the instructions in writing.

11. **Audit**

11.1. Vendor must make available to Plume all information necessary to demonstrate compliance with the obligations of Data Protection Law and this DPA and allow for and contribute to audits, including inspections, conducted by a Supervisory Authority, Plume or another auditor mandated by Plume.

11.2. Plume and Vendor each bear their own costs related to an audit. If an audit determines that the Vendor violated Data Protection Law or this DPA, then Vendor bears all costs related to the audit.

12. **Liability**

12.1. Vendor is fully liable to Plume and any Third-Party Controller for any infringements of Data Protection Law or this DPA by Vendor or Vendor's Processors.

12.2. Where Plume has paid damages or fines, Plume is entitled to claim back from Vendor that part of the compensation, damages or fines, corresponding to Vendor's part of responsibility for the damages or fines.

12.3. Vendor must indemnify Plume, its affiliates, directors, officers and personnel against all claims by third parties and resulting liabilities, losses, damages, costs and expenses (including reasonable external legal costs, administrative fines and other penalties) suffered or incurred by any of them, whether in contract, tort (including negligence) or otherwise arising out of or in connection with any infringement by Vendor or Vendor's Processors of this DPA or its obligations under Data Protection Law.

13. **Confidentiality**

13.1. Vendor must keep all Personal Data and all information relating to the Processing thereof, in strict confidence.

13.2. Vendor authorizes Plume to disclose the name(s) of Vendor and Vendor's Subprocessors to Third-Party Controllers, including by publishing a list on Plume's website.

14. **Notifications**

14.1. Vendor must make all notifications required under this DPA at least to Plume's Data Protection Officer / Legal Department via email to legal@plume.com

14.2. Vendor must make all notifications relating to the security of the Processing to the contact identified in **Section 15.1** and to Plume's Chief Information Security Officer via email to infosec@plume.com.

15. **Term and duration of Processing**

15.1. The Processing will last no longer than the term of the Agreement.

15.2. Upon termination of the Processing, Vendor must, at Plume's choice, delete or return all Personal Data and must delete all remaining copies within ninety (90) days after confirmation of Plume's choice.

15.3. This DPA is terminated upon Vendor's deletion of all remaining copies of Personal Data in accordance with **Section 16.2**.

16. **Applicable law and jurisdiction**

16.1. This DPA is governed by the laws of Slovenia. Any disputes relating to this DPA will be subject to the exclusive jurisdiction of the courts of Ljubljana, Slovenia.

17. **Modification of this DPA**

17.1. This DPA may only be modified by a written amendment signed by both Plume and Vendor.

18. **Invalidity and severability**

18.1. 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	**Vendor**
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

Plume authorizes Vendor to engage the following Subprocessors:

#	Name	Description

APPENDIX 1

DESCRIPTION OF THE PROCESSING

1. **Data Subjects**

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

#	Category	Description

2. **Categories of Personal Data**

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

#	Category	Description

3. **Sensitive Data**

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

#	Category	Description

4. **Processing operations**

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

#	Operation	Description

APPENDIX 2

SECURITY MEASURES

Vendor and Data Importer will, at a minimum, 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 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;
- ☐ Creation of *one* master record per user, user-master data procedures per data processing environment; and
- ☐ Encryption of archived data media.

3. **Data access control**

Technical and organizational measures 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; and
- ☐ Encryption.

4. **Disclosure control**

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

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