Plume

PROVIDER DATA PROCESSING ADDENDUM

This Provider Data Processing Addendum ("**Provider DPA**") forms part of the Plume Services and Distribution Agreement for the Plume Services ("**Agreement**") made by and between Plume Design, Inc. ("**Plume**") and the internet or communications services provider named in the Agreement ("**Provider**"). This Provider DPA is effective on the date signed by both Plume and Provider ("**DPA Effective Date**").

1. **Definitions.** Capitalized terms used in this Provider DPA have the meanings given in this Section 1.

1.1. "**Controller**" means the organization that determines the purpose and means of Processing of Personal Information.

1.2. "**Data Protection Laws**" means applicable laws and legal requirements relating to privacy and the collection, disclosure, disposal, retention, security, transfer and other Processing of Personal Information pursuant to the Agreement, each as amended, repealed, consolidated or replaced from time to time.

1.3. "**Data Subject**" means an identified or identifiable natural person to whom Personal Information relates (and an entity when an entity is treated similarly to a natural person under Data Protection Laws); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.

1.4. "**Data Subject Rights**" means rights available to Data Subjects under Data Protection Laws that are applicable to Personal Information Processed pursuant to the Agreement.

1.5. "**Personal Information**" means any information subject to Data Protection Law that identifies or could be used to identify a Data Subject and is Processed in relation to the Agreement

1.6. "**Personal Information Breach**" means any accidental or unlawful acquisition, destruction, loss, alteration or other unauthorized Processing of or access to Provider Personal Information.

1.7. "**Plume Privacy Policy**" means the Privacy Policy, available at https://www.plume.com/legal/privacy/, as amended from time to time in accordance with its terms.

1.8. "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Information, whether or not by automated means.

1.9. "**Processor**" means an entity that Processes Personal Information for and on behalf of a Controller.

1.10. "**Provider Personal Information**" means Personal Information that (i) is subject to Data Protection Laws, (ii) is Processed for purposes of performing the Plume Services pursuant to the Agreement and (iii) is Customer Data or for which Provider is Controller. Provider Personal Information does not include Services Data.

1.11. "**Restricted Transfer**" means a cross-border transfer or other disclosure of Provider Personal Information that is restricted by Data Protection Laws because the disclosure is made to a person or entity located in a jurisdiction which a competent government authority has determined does not ensure the same or higher level of data protection as the jurisdiction from which the Provider Personal Information originates ("**Originating Jurisdiction**").

1.12. "**Sub-Processor**" means a Processor engaged by Plume (acting as a Processor) to Process Provider Personal Information for and on behalf of Provider as Controller.

Capitalized terms used but not defined in this Provider DPA (including Customer Data, Plume Services and Services Data) have the meanings given in the Agreement.

2. **Scope and Roles of the Parties.**

2.1. Scope of this Provider DPA. This Provider DPA applies to the Processing of Personal Information as required or permitted by this Provider DPA and the Agreement. The terms of this Provider DPA do not and will not apply to Plume's Processing of Personal Information that is exempt from Data Protection Laws or Processed by Plume as Controller.

2.2. Plume's Role as Processor. Provider is the Controller of Provider Personal Information and appoints Plume as a Processor. The subject matter, nature and purpose of the Processing, the types of Provider Personal Information Processed and the categories of Data Subjects are set out in Annex 1 to this Provider DPA and in the Agreement.

2.3. Plume's Role as Controller. Provider acknowledges that Plume is a separate and independent Controller when Plume Processes Services Data. If the Data Protection Law known as the California Consumer Privacy Act (as amended and regulations promulgated thereunder from time to time) ("**CCPA"**) applies, then the Parties expressly agree that, with respect to Provider, Plume is not a "third party" (as defined in CCPA) with respect to Processing of Services Data.

3. **Processing of Personal Information.**

3.1. Compliance with Data Protection Laws. Provider and Plume agree to comply with Data Protection Laws that apply to their respective roles and Processing activities.

3.2. Plume Privacy Policy, Consent, and Notice to Data Subjects. Provider must: (i) require that Customers and Data Subjects agree to the Plume End-User Terms or provisions equivalent to the Plume End-User Terms and (ii) obtain Data Subjects' consent to Processing of their Personal Information pursuant to the Agreement.

3.3. Plume's Processing of Provider Personal Information as a Processor.

a. When acting as a Processor pursuant to Section 2.2, Plume will Process Provider Personal Information: (i) to fulfill its obligations to Provider under the Agreement and this Provider DPA; (ii) to provide the Plume Services and related technical support in accordance with Provider's instructions (as documented by this Provider DPA, the Agreement, and any applicable statement of work or order form) ("**Instructions**"); and (iii) as further specified via authorized use of the Plume Services (including through settings and other functionality of the Plume Services) and customer support.

b. Unless prohibited by applicable law, Plume will inform Provider without undue delay if Plume becomes aware that any of the Instructions conflict with Data Protection Laws. Plume may Process Provider Personal Information other than as set forth in Instructions if required under applicable law to which Plume is subject. Plume will inform Provider in such a case prior to Processing, unless prohibited from doing so.

c. Plume will ensure that all personnel authorized to Process Provider Personal Information pursuant to this Provider DPA are subject to an obligation of confidentiality with respect to Provider Personal Information.

d. Taking into account the nature of the Processing and the information available to Plume, Plume will assist Provider with the fulfilment of Provider's own obligations under Data Protection Laws to: (i) respond to verifiable requests by Data Subjects (or their lawful representatives) for exercising their Data Subject Rights; (ii) conduct data protection impact assessments and prior consultations with competent government authorities when required by Data Protection Laws; and (iii) notify Provider of a Personal Information Breach. Unless prohibited by Data Protection Laws, Plume may charge a reasonable fee for assistance provided to Provider.

e. If Plume receives a Data Subject Request applicable to Provider Personal Information Processed by Plume, Plume will promptly redirect the individual to Provider.

f. If Plume is aware that Plume is Processing Provider Personal Information subject to the CCPA, then Plume, when acting as a service provider (as defined in the CCPA), will not: (i) sell or

share (as such terms are defined in the CCPA) any Provider Personal Information; (ii) retain, use or disclose Provider Personal Information for any purpose other than for the business purposes specified in the Agreement; or (iii) combine Provider Personal Information with Personal Information that Plume receives other parties or collects from Plume's own interaction with Data Subjects, in each case except as permitted by CCPA. By execution of this Provider DPA, Plume certifies that it understands the specific restrictions contained in this Section 3.3f.

4. **Security.** Taking into account the costs of implementation and Processing, Plume will implement appropriate technical and organizational measures to provide a level of security to Provider Personal Information reasonable and appropriate to the risk, including the measures listed in Annex 2 of this Provider DPA (collectively, "**Security Measures**") and as required by Data Protection Laws.

5. **Personal Information Breach**

5.1. Personal Information Breach Notification. Plume will provide notification to Provider without undue delay after Plume has a reasonable degree of certainty that a Personal Information Breach involving Provider Personal Information and subject to the Agreement has occurred ("**Personal Information Breach Notification**"), in each case as required under Data Protection Laws. Plume will deliver the Personal Information Breach Notification to the email address associated with the Plume account administrator or such other contact as Plume determines appropriate. Provider is responsible for ensuring that Plume has Provider's up-to-date contact information for purposes of Personal Information Breach Notifications. Provider agrees to notify Plume without undue delay if Provider becomes aware of any actual or likely misuse of Provider's accounts or Data Subjects' authentication credentials.

5.2. Responding to Personal Information Breach. After delivering the Personal Information Breach Notification, Plume will take steps it deems necessary to document, remediate and minimize the effects of the Personal Information Breach with respect to Provider Personal Information and to prevent recurrence.

5.3. Assistance with Personal Information Breach Obligations. Provider is solely responsible for complying with its obligations under Data Protection Laws with respect to a Personal Information Breach but Plume will reasonably assist Provider in Provider's compliance with Provider's Personal Information Breach-related obligations. Unless prohibited by Data Protection Laws, Plume may charge a reasonable fee for assistance provided to Provider.

5.4. Notification to Data Subjects and Others. Plume and Provider will work in good faith to mutually agree about whether and how Provider or Plume will fulfil notification obligations to Data Subjects or other third parties as required by Data Protection Laws and the timing and content of such notification and appropriate allocation of costs.

6. **Sub-Processing by Plume as Processor**

6.1. Use of Sub-Processors. When Plume is acting as a Processor, Provider hereby authorizes Plume to engage Sub-Processors to Process Provider Personal Information. A list of Plume's Sub-Processors as of the effective date of this Provider DPA is included in Annex 3 ("**Sub-Processor List**").

6.2. Sub-Processor Written Agreement. Plume (as Processor) will (i) take commercially-reasonable steps to select and retain Sub-Processors that are capable of maintaining appropriate privacy and security measures to protect Personal Information consistent with Data Protection Laws; (ii) require that each Sub-Processor complies with obligations that are no less restrictive than those imposed on Plume under this Provider DPA, to the extent applicable to the nature of the Plume Services provided by such Sub-Processor; and (iii) otherwise comply with Data Protection Laws, such as requirements for supervision of Sub-Processors to ensure protection of Personal Information. Plume is and will remain liable for the acts and omissions of its Sub-Processors to the same extent Plume (as Processor) would

be liable if performing the services of each Sub-Processor directly under the terms of this Provider DPA.

6.3. New Sub-Processors. Plume may from time to time appoint new or replacement Sub-Processors. At least fifteen (15) business days prior to any disclosure of Provider Personal Information to a new or replacement Sub-Processor, Plume will update the Sub-Processor List to include the new or replacement Sub-Processor. Provider may object in writing to a new or replacement Sub-Processor within fifteen (15) days after the date on which the Sub-Processor List is updated, which objection must provide a reasonably-detailed explanation for the objection. Provider and Plume will use good-faith efforts to agree on a replacement for the objected-to Sub-Processor. If the parties are unable to agree on the new or replacement Sub-Processor within forty five (45) days, then Provider or Plume may, upon written notice to the other party, terminate that part of the Agreement that relates to the services provided by the objected-to Sub-Processor.

7. **Audit**

7.1. Documentation. Plume makes available audit reports, documentation and other compliance information ("**Documentation**") for Provider upon request.

7.2. Assistance with Audits. If the Documentation does not meet the audit requirements for Plume's Processing of Provider Personal Information allowed to Provider under Data Protection Laws, then Plume will make available to Provider all such additional information necessary to demonstrate compliance with this Provider DPA and allow for and contribute to audits or inspections ("**Provider Audit**"), in each case as required by Data Protection Laws or as reasonably requested by Provider and performed by an independent auditor mutually agreeable to Provider and Plume. Unless mandated by Data Protection Laws or a competent government authority, Provider may not request the performance of a Provider Audit more than once per calendar year during the term of the Agreement and must notify Plume no less than forty-five (45) calendar days prior to any Provider Audit. Plume may suspend any Provider Audit or withhold requested information until Plume has confirmed the lawfulness of the Provider Audit. Provider acknowledges and agrees that a Provider Audit will not oblige Plume to provide Provider or its auditor with access to information pertaining to Plume's internal pricing information or other recipients of Plume's products or services or Plume's employees. Each Provider Audit will be subject to Plume's reasonable policies and procedures for the purposes of preserving security and confidentiality. Where permitted by Data Protection Laws, Provider bears all costs related to audits and inspections under this Provider DPA.

7.3. Prior to a Provider Audit conducted by a third party on Provider's behalf, Provider will require that all of the third party's personnel execute a confidentiality agreement with Plume that requires the third party's personnel to (i) use information accessed during the Provider Audit solely for purposes of performing the Provider Audit and (ii) handle that information in accordance with the same procedures that apply to Plume's handling of its own confidential information as described in the relevant provision of the Agreement.

8. **Restricted Transfers.** Plume agrees to comply with Data Protection Laws with respect to any Restricted Transfer. Plume agrees to work in good faith with Provider to enter into additional contractual provisions with respect to a Restricted Transfer as and when required by Data Protection Law, including as set forth in Annex 4. If Plume Processes Provider Personal Information subject to the GDPR, Provider authorizes Plume to transfer such Provider Personal Information to a country outside the EEA.

9. **Changes in Data Protection Laws.** The Parties may notify each other in writing from time to time of any variation to this Provider DPA due to an actual or likely conflict resulting from a change in Data Protection Laws. If necessary, the Parties agree to work in good faith to amend this Provider DPA to allow either party to comply with Data Protection Laws or other applicable laws, including in particular with respect to Restricted Transfers.

10. **Termination; Return or Deletion of Provider Personal Information.** This Provider DPA is terminated upon the termination of the Agreement. Provider may request that Plume, as a Processor of Provider Personal Information, returns or destroys Provider Personal Information up to ninety (90) days after termination of the Agreement. If law applicable to Plume requires storage of Provider Personal Information after Provider has made its election to have Plume return or delete Provider Personal Information, Plume will notify Provider and store Provider Personal Information in compliance with the relevant terms of this Provider DPA until Plume can lawfully destroy the Provider Personal Information.

11. **General Provisions**

11.1. Notifications**.** Provider will send all notifications, requests and Instructions under this Provider DPA to Plume via email to privacy@plume.com.

11.2. Liability. Provided that Plume's liability is limited as set out in the Agreement, 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 that correspond to Provider's part of responsibility for the damages or fines.

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

11.4. Order of Precedence**.** If a term of this Provider DPA and a term of the Agreement conflict, then the term of this Provider DPA will prevail with respect to the Processing of Provider Personal Information. If requirements set forth in Annex 4 of this Provider DPA for a Restricted Transfer apply in connection with any Restricted Transfer and any term of this Provider DPA conflicts with requirements in Annex 4, then the applicable requirements in Annex 4 will prevail.

11.5. Interpretation and Construction. Any ambiguity in this Provider DPA will be resolved to permit Provider and Plume to comply with Data Protection Laws. Headings used in the Provider DPA are for convenience only and will not be construed to alter the meaning of any terms of this Provider DPA. Statutory references will be deemed to correspond to the provision in effect or as amended from time-to-time. The English language version of this Provider DPA shall control.

11.6. Amendments. Except as required under Section 9, no amendment to this Provider DPA is effective unless it is in writing in accordance with Section 11.7, identified as an amendment to this Provider DPA and signed by an authorized representative of each party to this Provider DPA

11.7. Counterparts. This Provider DPA may be executed in counterparts, by manual, facsimile, email (via signed .pdf documents exchanged via email), or electronic signature, each of which will be deemed an original and all of which together will constitute one and the same instrument.

11.8. Survival. The provisions of this Provider DPA survive the termination or expiration of the Agreement for as long as Plume Processes Provider Personal Information.

[Signature Page follows]

[Signature Page to Provider DPA]

PLUME	**PROVIDER**
Name:	Name:
Title:	Title:
Email:	Email:
Plume Legal Name:	Provider Legal Name:
Provider Address:	Provider Address:
Signature:	Signature:
Date:	Date:

PROVIDER DATA PROCESSING ADDENDUM

ANNEX 1: DESCRIPTION OF PROCESSING - WORKPASS AND HOMEPASS

1. Data Subjects

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

Category
Personnel of Provider or a Customer who use the Plume Services and end users of the Plume Services

2. Categories of Provider Personal Information

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

	Category
1.	Accounts ● First Name, last name or system generated name ● Clear name or system generated name (Plume may not receive end users' names but instead receive a system generated unique "ID). ● (Login) email address ● Account ID ● Provider ID ● Email address, email ID ● "Plume Partner ID" for each Provider ● Password ● WorkPass Only: Year of birth, gender (optional), telephone number, profile photo (optional) and social media handle (optional)
2.	Location ● Region/Jurisdiction (e.g., US, UK, EU, SG, JP) based on GeoIP ● Name, time of account creation and on-boarded ● GeoIP, WAN IP, latitude, longitude (generated from use of mobile app) ● City, state/province, postal code, country ● Time zone ● Internet Service Provider
3.	Network Configuration ● Internet Service Provider ● Network status (online/offline/partial), time of each network status. (Indicates the networking addresses of the devices and systems used to communicate with Plume and the internet along with the operating statistics of the WiFi and internet connections.) ● WiFi settings ● WiFi SSID, key ● WiFi encryption mode ● Primary/secondary DNS ● DHCP Reservations, port forwarding. Static IP assignments to client devices, port forwarding rules from router to client devices.
4.	Customer Network Topology – HomePass and WorkPass ● Access zones ● Passwords ● Policies ● Location ID ● WiFi SSID ● PSK ● PSK zone

	Category
	● PSK assignment ● PSK status ● PSK expiry
5.	Profiles for Customer and Customer's end users: ● Profile ID ● Name of person in profile ● Primary Device of person in profile ● Assigned Devices of person in profile ● Profile phot (optional) ● When user was last in range of Customer Network
6	Parental Controls - HomePass: ● "freeze" policy for devices connected to the Customer Network
7	Nodes (CPE Access Points): ● Nickname ● Model ● ID, location and Customer with which the node is associated ● 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 ● Volume of data consumption of the Customer's end users' devices and CPE nodes (transmitted/ received bytes). ● Steering History – including WAN IP, MAC Address, Hostname, Nickname ● Network topology data. (This data depicts the connections between devices in use and the Plume network access points serving WiFi, including radios/ channels and connection state.
10	Service statistics and Logs Speed Test ● Speed Test Results – ISP, ISP speeds, Outages, Upload and Download speeds history App Usage Analytics ● Plume Mobile App (iOS / Android) usage stats (Features used / Screen views) ● Provider ID ● Location ID ● First Name ● Last Name ● Email ● City ● State ● Country

	Category
	● 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 connected devices, device inventory data, and software and hardware versions. ● Server Logs from 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 and Port, Protocol, Packets and Byte counts) and App Time Online detected from IP Flows.
12	Information regarding disruptions in WiFi waves in the periphery of the Plume network access points and devices connected to the Plume network - HomePass Only: ● Configuration of Sounding Devices ● Live motion per location ● Motion Density history (entire network) ● Home Security Events ● State History
13	Crash Reports Crash reports. Plume collects crash reports for both the Plume Software and the Plume App. These reports 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 Information Processed concern the following special categories of Personal Information (please specify):

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

4. Processing operations

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

	Operation
1.	Sharing between Provider and Plume to enable Plume to compute, store and continuously refine algorithms used to provide the Plume Services.
2.	Processing as necessary 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 a user account, ● verifying user identity , ● communicating via the Plume App, ● providing customer support,

	Operation
	● arranging the delivery or other provision of products and services or their updates, ● identifying devices, e.g. to more accurately represent these devices to Customer 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 Provider, including troubleshooting. HomePass Only ● displaying live motion visuals and motion history ● displaying time spent by users on various Internet applications (app time usage detection), ● alerting users about 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 and helping prevent connected devices from unauthorized access.
3.	To comply with applicable laws regarding the Processing of Personal Information on behalf of the Provider as described above and governed by this Provider DPA.
4.	To protect the safety, integrity, rights, or security of users, the Plume Services or equipment, or any third party.
5.	To ensure compliance with the regulatory requirements for the specific region.

[***END OF ANNEX 1***]

PROVIDER DATA PROCESSING ADDENDUM

ANNEX 2: SECURITY MEASURES

Plume's Security Measures are designed to: (a) protect the confidentiality, integrity, and availability of Provider Personal Information in Plume's possession or control or to which Plume has access; (b) protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Provider Personal Information; (c) protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Provider Personal Information; (d) protect against accidental loss or destruction of, or damage to, Provider Personal Information. The Security Measures include:

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 Information 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 Provider Personal Information in accordance with their access rights, and that Provider Personal Information 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 Information without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure; and
- Encryption.

4. **Disclosure control**

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

- Logging; and
- Transport security.

5. Entry control
Technical and organizational measures to monitor whether Provider Personal Information 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. Contractual controls
Technical and organizational measures to ensure that Provider Personal Information are Processed solely in accordance with the Agreement and this Provider DPA (including Instructions).

7. Availability control
Technical and organizational measures to ensure that Provider Personal Information 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 Provider Personal Information 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.

[***END OF ANNEX 2***]

PROVIDER DATA PROCESSING ADDENDUM

ANNEX 3: SUB-PROCESSORS

Plume maintains its Sub-Processors List at https://www.plume.com/legal/subprocessors/

[***END OF ANNEX 3***]

Plume

PROVIDER DATA PROCESSING ADDENDUM

ANNEX 4: RESTRICTED TRANSFERS

Plume agrees to the following contractual clauses and other requirements with respect to Restricted Transfers. Provider's signature on this Provider DPA will be deemed to constitute Provider's signature and acceptance of the relevant contractual terms set forth below and incorporated into this Provider DPA and the Agreement. Accordingly, the parties to the relevant contractual terms will be the same as the parties to the Provider DPA unless otherwise agreed in writing.

Restricted Transfers Subject to GDPR
When Provider as a Controller ("data exporter") makes a Restricted Transfer of Provider Personal Information subject to GDPR to Plume ("data importer") (i) to a jurisdiction that is not part of the European Economic Area and not covered by an adequacy decision under GDPR Article 45 and (ii) the Plume's Processing of Provider Personal Information is not otherwise protected by appropriate transfer mechanisms as specified under Chapter V of the GDPR, then data exporter and data importer agree to complete and execute the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("**Standard Contractual Clauses**") (*Module Two*).

The parties agree that the Standard Contractual Clauses (*Module Two*) set forth in Annex 4-1 below.

If Provider as a Controller makes a Restricted Transfer of Provider Personal Information subject to GDPR to Plume as a separate and independent Controller located in a non-EEA jurisdiction which is not covered by an adequacy decision under GDPR Article 45 and Plume's Processing of Provider Personal Information is not otherwise protected by appropriate transfer mechanisms as specified under Chapter V of the GDPR, then the parties agree to complete and execute the Standard Contractual Clauses (*Module Three*).

The Standard Contractual Clauses also will apply to a Restricted Transfer when the relevant Provider Personal Information is not subject to GDPR but the Originating Jurisdiction's competent government authority for that Provider Personal Information authorizes the use of the Standard Contractual Clauses.

Restricted Transfers Subject to Swiss Data Protection Law. When Provider ("data exporter") makes a Restricted Transfer of Provider Personal Information to Plume ("data importer") subject to the Federal Data Protection Act of Switzerland ("**FADP**") and the data importer is located outside Switzerland or the EEA and or jurisdiction not covered by the list published by the Federal Data Protection and Information Commissioner of Switzerland (available at https://www.fedlex.admin.ch/eli/cc/2022/568/de#annex_1), then data exporter and data importer agree to complete and execute the Standard Contractual Clauses (*Module Two*) subject to the following:

(i) if the Restricted Transfer of Provider Personal Information is subject to the FADP but *not* also covered by GDPR, then the following terms will be deemed to amend the Standard Contractual Clauses:

- All references to the GDPR are to be understood as references to the FADP;
- The competent supervisory authority in Annex I.C under Clause 13 is the Federal Data Protection and Information Commissioner of Switzerland;
- Applicable law for contractual claims under Clause 17 is the law of Switzerland;
- The term "Member State" must not be interpreted in such a way as to exclude a data subject in Switzerland from the possibility of suing for his/her rights in Switzerland in accordance with Clause 18 c.; and
- Data of Swiss legal entities are subject to protection as personal data of data subjects under FADP.

(ii) if the Restricted Transfer of Provider Personal Information is subject to the FADP *and* GDPR, then the following terms will be deemed to amend the Standard Contractual Clauses:

- The competent supervisory authority in Annex I.C under Clause 13 will include the Federal Data Protection and Information Commissioner of Switzerland; and
- The term "Member State" must not be interpreted in such a way as to exclude a data subject in Switzerland from the possibility of suing for his/her rights in Switzerland in accordance with Clause 18c.

Restricted Transfers Subject to UK GDPR. For a Restricted Transfer subject to the United Kingdom's Data Protection Act 2018 ("**UK GDPR**"), the parties agree that the International Data Transfer Addendum to the Standard Contractual Clauses set forth in Annex 4-2 below will apply.

Restricted Transfers from Australia. Provider authorizes Plume to transfer Provider Personal Information to a third party in a jurisdiction outside of Australia if the Restricted Transfer is permitted under APP 8 in the Privacy Act.

Restricted Transfers from Canada. To the extent that Plume Processes Provider Personal Information of Data Subjects located in Canada, Plume will not share, transfer, disclose or otherwise provide access to that Provider Personal Information for any third party unless Provider has authorized Plume to do so in writing or as permitted by the Agreement and Data Protection Laws. Provider hereby authorizes Plume to share, transfer, disclose or otherwise provide access to Provider Personal Information to Sub-Processors that Process Provider Personal Information. Provider hereby acknowledges that Plume may Process Provider Personal Information outside of Canada, including the in European Economic Area and United States, in each case in compliance with Data Protection Laws.

Restricted Transfers from Japan. To the extent that Plume Processes Provider Personal Information of Data Subjects located in Japan, Provider authorizes Plume to transfer that Provider Personal Information to a third party in a jurisdiction outside of Japan only if: (i) the jurisdiction in which the recipient is located has a legal system that is deemed equivalent to the Japanese data protection regime as designated by the PPC; (ii) the recipient has adequate measures for the protection of Provider Personal Information, as specified by the PPC; (iii) the Data Subject consents to the Restricted Transfer; or (iv) the Restricted Transfer is otherwise permitted under Japan's Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in thereafter) ("**APPI**"). When providing Provider Personal Information to a Sub-Processor or other third party outside Japan, Plume will, when required by the PPC (i) take necessary measures as specified by the PPC to ensure the continuous implementation of measures equivalent to the terms of this Provider DPA by such third party and provide information about such necessary measures to the relevant Data Subject upon his/her request; and (ii) provide information regarding the Personal Information protection system in the jurisdiction in which the third party is located, the measures taken by the third party to protect Provider Personal Information, and other relevant information to the Data Subject in advance, as required by the PPC.

Where required under the APPI, Provider will obtain consent from those individuals for Provider's transfer of their Personal Information outside Japan, including to the United States where Plume is located and on behalf of Plume for Plume's transfer of their Personal Information to the countries where Plume's Sub-Processors reside as listed in the Sub-Processor List, as amended from time to time.

Restricted Transfers from Other Jurisdictions. To the extent that Plume Processes Personal Information of Data Subjects located in other jurisdictions and is subject to the Data Protection Laws of that jurisdiction, Plume will Process Personal Information in accordance with the requirements of the Data Protection Laws.

ANNEX 4 -1

STANDARD CONTRACTUAL CLAUSES
SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and €;

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Module Two: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall,

where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for,

in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities –

relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: *The entity identified as Provider in the Agreement.*

Address: *The address of the Provider specified in the Agreement.*

Contact person's name, position and contact details:

The contact details of the Provider specified in the Agreement.

Activities relevant to the data transferred under these Clauses:

The performance of the Plume Services pusuant to the Agreement.

Signature and date:

PROVIDER

Name:
Title:
Signature:
Date:

Role (controller/processor): *Controller*

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: *Plume Design, Inc. or the entity identifed as Plume in the Agreement.*

Address*: 325 Lytton Ave, Palo Alto, CA 94301*

Contact person's name, position and contact details:

Shari Pire, Chief Legal and Sustainability Officer, spire@plume.com

Activities relevant to the data transferred under these Clauses:

The data importer provides the Plume Services pursuant to the Agreement.

Signature and date:

PLUME

Name:
Title:
Signature:
Date:

Role (controller/processor): *Processor*

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Annex 1 to the Provider DPA.

Categories of personal data transferred

See Annex 1 to the Provider DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

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

Data is transferred as often as necessary in order to perform the Plume Services

Nature of the processing

See Annex 1 to the Provider DPA.

Purpose(s) of the data transfer and further processing

Personal data are transferred in order to perform the Plume Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Unless required or permitted by applicable law or otherwise requested by the data exporter, Plume as the data importer will delete personal data within ninety (90) days after returning personal data.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Plume may engage sub-processors to assist with providing the Plume Services and the subject matter, nature and duration of the processing by any of Plume's sub-processor will be materially equivalent to the subject matter, nature and duration of the processing carried out by Plume.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

Supervisory Authority of the Republic of Ireland.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Plume's Security Measures are designed to protect the confidentiality, integrity, and availability of Provider Personal Information in Plume's possession or control against anticipated threats or hazards, against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Provider Personal Information and accidental loss or destruction of, or damage to, Provider Personal Information. The Security Measures include:

1. PHYSICAL ACCESS CONTROL

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available on premises and in facilities (including databases, application servers, and related hardware), where Provider Personal Information is 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 use 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 Provider Personal Information in accordance with their access rights, and that Provider Personal Information 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 Information without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure; and
- Encryption.

4. **DISCLOSURE CONTROL**

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

- Logging; and
- Transport, transmission and storage security.

5. ENTRY CONTROL

Technical and organizational measures to monitor whether Provider Personal Information 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. CONTRACTUAL CONTROLS

Technical and organizational measures to ensure that Provider Personal Information is Processed solely in accordance with the Agreement and the Provider DPA (including instructions).

Technical and organizational measures to ensure that Provider Personal Information is Processed solely in accordance with the instructions of the Provider include:

- Unambiguous wording of the contract
- Formal commissioning (request form)

7. AVAILABILITY CONTROL

Technical and organizational measures to ensure that Provider Personal Information 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 Provider Personal Information 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

Plume may engage sub-processors to assist with providing the Plume Services and those sub-processors' specific technical and organisational measures will be materially equivalent to the technical and organisational measures taken by Plume.

ANNEX III – LIST OF SUB-PROCESSORS

Plume maintains its Sub-Processors List at https://www.plume.com/legal/subprocessors/.

[***END OF ANNEX 4-1***]

ANNEX 4 -2

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	DPA Effective Date	
The Parties	Provider as Exporter (which sends the Restricted Transfer)	Plume as Importer (which receives the Restricted Transfer)
Parties' details	As set forth in the Provider DPA and Agreement	As set forth in the Provider DPA and Agreement: Plume Design, Inc. 325 Lytton Ave Palo Alto, CA 94301
Key Contact		Plume Design, Inc. 325 Lytton Ave Palo Alto, CA 94301 Shari Pire, Chief Legal and Sustainability Officer, spire@plume.com

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs set forth in Annex 4 to the Provider DPA.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties) and which for this Addendum is set out in:

Annex 1A: List of Parties	The Parties are set forth in Table 1 to this Addendum.
Annex 1B: Description of Transfer	Annex 1 to the Provider DPA and the Approved EU SCCs sets out the description of Processing for this Addendum.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data	Annex 2 to the Provider DPA and the Approved EU SCCs shall serve as ANNEX II to this Addendum.
Annex III: List of Sub processors (Modules 2 and 3 only)	Annex 3 to the Provider DPA and the Approved EU SCCs shall serve as ANNEX III to this Addendum.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

- **Interpretation of this Addendum**

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs to which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.
19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
    a. its direct costs of performing its obligations under the Addendum; and/or
    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
20. The Parties do not need the consent of any third party to make changes to this Addendum but any change must be made in accordance with its terms.

[***END OF ANNEX 4***]