# ALTERYX DATA PROCESSING AGREEMENT

## 1. Introduction

This Alteryx Data Processing Agreement ("**DPA**") is hereby incorporated by reference into and is part of the End User License Agreement or Master License Agreement, as applicable, between Licensee and Alteryx (together with its Affiliates, "**Alteryx**") ("**Agreement**") solely to the extent and for the purposes outlined herein. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. In the event of a conflict between the Agreement and this DPA, this DPA (together with the Standard Contractual Clauses) shall control.

a) Notwithstanding the foregoing, to the extent permitted by applicable law, any claims brought under or in connection with this DPA shall be subject to the exclusions and limitations set forth in the Agreement.

b) Except as expressly permitted by the Standard Contractual Clauses, no one other than a party to this DPA, its successors and permitted assigns shall have any right to enforce any of its terms.

c) For Licensee and those entities Licensee permits to use the Licensed Products, Licensee acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data contained in Licensee Content in accordance with this DPA, including, where applicable, Licensee's use of Alteryx as a Data Processor. Where Alteryx informs or gives notice to Licensee, such information or notice is deemed received by those entities permitted by Licensee to use the Licensed Products and it is Licensee's responsibility to forward such information or notices to such entities.

d) The provisions of this DPA and the Standard Contractual Clauses only apply to the extent that Alteryx processes Personal Data as part of Licensee Content pursuant to the Agreement and shall terminate simultaneously and automatically with deletion of all Licensee Content following termination or expiration of the Agreement.

## 2. Definitions

Capitalized terms have the meaning given to them in the Agreement, unless otherwise defined below.

a) "**Applicable Law**" means the relevant data protection and data privacy laws, rules, and regulations directly applicable to this DPA and the Personal Data included in Licensee Content, as outlined in Annex I to the Standard Contractual Clauses, including, but not limited to, the General Data Protection Regulation (EU 2016/679) ("**GDPR**") and the California Consumer Privacy Act ("**CCPA**").

b) "**Licensee Content**" means any data or information that Licensee uploads, connects to, or imports into the Licensed Products, including Cloud Services, from its internal data sets or other sources not supplied by Alteryx (*e.g.*, Licensee-Sourced Data) to facilitate Licensee's use of such Licensed Products or Cloud Services. For the avoidance of doubt, Licensee Content is considered "Licensee-Sourced Data" under the Agreement. Usage Data is expressly excluded from Licensee Content.

c) "**Licensed Products**" means those Alteryx products and services referenced in the Agreement and any Order Form attached thereto.

d) "**Personal Data**" shall have the meaning assigned to the terms "personal data", "personally identifiable information", or "personal information" under Applicable Law.

e) "**process**", "**processes**", "**processing**" and "**processed**" means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

f) "**Security Incident**" means any confirmed unauthorized or unlawful breach of security that leads to the accidental or unauthorized destruction, loss, alteration, disclosure of or access to Personal Data included in Licensee Content.

g) "**Subprocessor**" means contractors, vendors and third-party service providers engaged by Alteryx that process Licensee Content.

**3. Data Handling, Access and Processing**

a) Role of the Parties. As between Licensee and Alteryx, Licensee is the Data Controller and Alteryx is the Data Processor solely with respect to any Personal Data contained in Licensee Content. For the avoidance of doubt, where Alteryx acts as a Data Controller of any Personal Data under Applicable Law, processing undertaken in its capacity as a Controller shall not be subject to this DPA.

b) CCPA. The Parties acknowledge and agree that Alteryx is deemed to be, and is acting as, a "Service Provider" (as such term is defined by the CCPA) to Licensee in connection with Alteryx's processing of Personal Data contained in Licensee Content pursuant to this DPA. The Parties understand and agree that Alteryx does not provide Licensee with monetary or other valuable consideration in exchange for the Personal Data contained within Licensee Content. Except as required by applicable law or regulation, Alteryx will not collect, access, use, disclose, process, or retain Personal Data contained in Licensee Content for any purpose other than providing the Licensed Products or another business purpose permitted by 11 CCR § 999.314(c), this DPA or the Agreement. Alteryx will not sell (as defined by Applicable Law, including, to the extent applicable, the CCPA) any Personal Data subject to this DPA.

c) General Compliance by Alteryx. Alteryx will process Licensee Content in material compliance with this DPA and Applicable Law.

d) General Compliance by Licensee. Licensee agrees that (i) it shall materially comply with its obligations as Controller of Licensee Content under Applicable Law, including with respect to its processing of Personal Data and any instructions it issues to Alteryx, and (ii) it has provided notice and obtained (or shall obtain) all necessary consents and rights under Applicable Law for Alteryx to process Personal Data pursuant to this DPA.

e) Subprocessors. The Standard Contractual Clauses shall govern Alteryx's use of Subprocessors for the purposes of this DPA. Alteryx shall update the list of Subprocessors engaged in processing License Content, found at https://www.alteryx.com/subprocessors, at least thirty (30) days in advance of adding a new Subprocessor. To receive notice via email, Licensee must subscribe to Subprocessor updates. If Licensee does not subscribe to such notices, Alteryx's posting of the name of such Subprocessor on its website will be deemed to constitute notice to Licensee in accordance with this provision. Licensee will have fifteen (15) calendar days to object to a Subprocessor in writing after notice is given. In the event Licensee objects within such 15-day period, Alteryx will make commercially reasonable efforts to address Licensee's good faith objection based on data privacy concerns, or, where feasible, to suggest a commercially reasonable change to avoid processing of the Personal Data by the objected-to Subprocessor.

f) Controller Instructions. Alteryx will process Licensee Content in accordance with Licensee's written instructions and as outlined in **Schedule 1**. Alteryx is not responsible for understanding or applying any laws, regulations, or industry standards specific to Licensee's industry or Licensee Content. The Parties agree that this DPA and the Agreement set out Licensee's complete and final instructions with regard to Alteryx's processing of Personal Data contained in Licensee Content. Any processing of Personal Data outside the scope of these instructions (if any) will require a signed written amendment to this DPA.

g) Data Subject Requests. Alteryx may (i) provide Licensee with self-service options or, (ii) solely to the extent that Licensee is unable to satisfy any data subject request pertaining to Licensee Content, provide reasonable assistance to Licensee to comply with its obligations as a Data Controller under Applicable Law.

**4. International Transfers**

a) Datacenter locations. Except as expressly agreed in writing, Alteryx may transfer and process Licensee Content, including any Personal Data contained therein, anywhere in the world where Alteryx, its Affiliates or its Subprocessors maintain data processing operations, provided that such processing complies with the requirements of Applicable Law. Specifically, Alteryx may store or otherwise process Licensee Content within the United States, regardless of the country in which Licensee is based or the country of origin for Licensee Content.

b) Transfers from the EEA. To the extent that Personal Data contained within Licensee Content is transferred by or on behalf of Licensee (including onward transfers) from within the European Economic Area (EEA) to Alteryx in a jurisdiction outside of the EEA, the Parties agree that, with respect to any restricted transfer under the GDPR, the Standard Contractual Clauses approved by the European Commission under Decision 2021/914 of 4 June 2021 shall provide the appropriate safeguards required of such transfer, subject to the following modifications:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9(a), Option 2 will apply, in accordance with any additional requirements outlined herein;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and will be governed by German law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Germany;

(vii) Annex I shall be deemed completed with the information set out in **Schedule 1** to this DPA; and

(viii) Annex II shall be deemed completed with the information set out in **Schedule 2** to this DPA.

c) Transfers from the United Kingdom or Brazil. To the extent that Personal Data contained within Licensee Content is transferred by or on behalf of Licensee (including onward transfers) from within the United Kingdom or Brazil to Alteryx in a jurisdiction outside of the same (each a "Restrictive Jurisdiction"), the Parties agree that, with respect to any restricted transfer under Applicable Law, the Standard Contractual Clauses approved by the European Commission under Decision 2010/87 of 5 February 2010 shall provide the appropriate safeguards required of such transfer, subject to the following modifications:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Applicable Law of the Restrictive Jurisdiction;

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Applicable Law of the Restrictive Jurisdiction;

(iii) references to "EU", "Union" and "Member State" shall be replaced with references to the Restrictive Jurisdiction;

(iv) the "competent supervisory authority" shall be the UK Information Commissioner or Brazil's National Data Protection Authority, as applicable;

(v) the "competent courts" shall mean the courts of England or Brazil, as applicable;

(vi) in Clause 9 and Clause 11(3), the SCCs shall be governed by the laws of England or Brazil, as applicable;

(vii) Appendix 1 shall be deemed completed with the information set out in **Schedule 1** to this DPA; and

(viii) Appendix 2 shall be deemed completed with the information set out in **Schedule 2** to this DPA.

(d) Alternative Transfer Mechanism. The Parties agree that the Standard Contractual Clauses shall not apply if and to the extent that Alteryx adopts an alternative mechanism for the lawful transfer of Personal Data under Applicable Law, in which event, the alternative mechanism shall apply instead.

**5. Information Security Program**

a) Alteryx agrees to maintain appropriate technical and organizational measures designed to protect Personal Data as required by Applicable Law (the "**Information Security Program**") and as outlined in Schedule 2. Further, Alteryx agrees to regularly test, assess and evaluate the effectiveness of its Information Security Program to ensure the security of the processing of Licensee Content.

b) Licensee is solely responsible for reviewing the information made available by Alteryx relating to data security and making an independent determination as to whether processing by Alteryx pursuant to the Agreement meets Licensee's requirements and its legal obligations under applicable law. Licensee acknowledges that the Information Security Program may be updated or modified from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Licensed Products.

c) Licensee agrees that, except as provided by this DPA, Licensee is responsible for its secure use of the Licensed Products, including securing its account authentication credentials, protecting the security of Licensee Content when in transit to and from the Licensed Products, and taking any appropriate steps to securely encrypt or backup any Licensee Content.

**6. Audits**

In the event of Licensee's reasonable and good faith belief that Alteryx is not in compliance with Applicable Law with respect to the processing of Personal Data contained in Licensee Content, Alteryx agrees to reasonably cooperate with Licensee, as outlined below.

a) Licensee may request assurance of Alteryx's compliance with its Data Processor obligations upon at least thirty (30) days' prior, written notice through the submission of security questionnaires or a request for the most recent third-party certification or summary executive findings pertaining to Alteryx's Information Security Program. Requests made under this Section 6a are limited to one per rolling calendar year.

b) Solely to the extent permitted by the applicable Standard Contractual Clauses, Licensee may, at Licensee's expense, request reasonable supplementary information through a remote audit of the Information Security Program and Alteryx's related policies and procedures.

**7. Deletion of Licensee Content**

a) Within sixty (60) days following termination or expiration of the Agreement for any reason, Alteryx will delete all License Content in its possession or control, excepting to the extent Alteryx is required by applicable law to retain some or all License Content.

b) Notwithstanding the foregoing, where expressly designated in the Agreement, Alteryx may provide Licensee a specified period following termination or expiration during which Licensee may backup or export Licensee Content. Following any such specified period of retention for Licensee's benefit, Alteryx will delete all License Content without further notice or obligation to retain such data.

**8. Security Incident**

a) Security Incident Procedure. Alteryx will implement and maintain policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to suspected or known Security Incidents, mitigate harmful effects of Security Incidents, and document Security Incidents and their outcomes, and (ii) restore the availability or access to Licensee Content in a timely manner.

b) Notice. Alteryx agrees to provide prompt written notice to Licensee, without undue delay and within the time period required under Applicable Law, if it knows or suspects that a Security Incident has taken place. To the extent known by Alteryx, such notice will include all available details required under Applicable Law to enable Licensee to comply with its notification obligations to regulatory authorities or individuals affected by the Security Incident. In any event, Alteryx will provide notices required by this Section 8 in the time and manner required by the Standard Contractual Clauses.

## Schedule 1

### A. LIST OF PARTIES

**Data exporter(s):**

*Name:* Licensee, as named in the Agreement

*Address:* See Agreement

*Contact person's name, position and contact details:* See Agreement

*Activities relevant to the data transferred under these Clauses:*

Upload to, storage of, and use of any Personal Data included in Licensee Content together with the Licensed Products for Licensee's benefit or the benefit of Licensee's employees, customers, and partners

*Role (controller/processor):* Controller

**Data importer(s):**

*Name:* Alteryx, Inc.

*Address:* 17200 Laguna Canyon Rd, Irvine, CA 92618 USA

*Contact person's name, position and contact details:*

Jennifer Sivan Davide

Senior Director, Privacy and Product Counsel and Data Protection Officer jennifer.davide@alteryx.com

*Activities relevant to the data transferred under these Clauses:*

Hosting of Licensee Content, which may, in Licensee's sole discretion, include Personal Data

*Role (controller/processor):* Processor

### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

Solely determined by Licensee as part of Licensee Content.

*Categories of personal data transferred*

Solely determined by Licensee as part of Licensee Content.

*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.*

Not permitted by the Agreement. Any use of the Licensed Products with Licensee Content that contains sensitive data is at Licensee's sole discretion.

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

Frequency of transfers of Licensee Content that include Personal Data are at Licensee's sole discretion in its use of the Licensed Products.

*Nature of the processing*

Hosting of Licensee Content, which may contain Personal Data, for Licensee's use of the Licensed Products.

*Purpose(s) of the data transfer and further processing*

Personal Data is transferred solely for Licensee's use of the Licensed Products with Licensee Content and for no further processing by Alteryx.

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

Users may delete their content at any time using self-service; Licensee may request the deletion of Licensee Content by opening a support request. All Licensee Content is retained for so long as Licensee continues to use the Licensed Products but is deleted within 60 days following termination of the Agreement.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing* Subprocessors engaged to process License Content are found at https://www.alteryx.com/subprocessors. Written agreements with Subprocessors require purging of data within 60 days following termination of the agreement, though most data is purged within one day following deletion by a customer.

### C. COMPETENT SUPERVISORY AUTHORITY

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

Bavarian State Office for Data Protection Supervision

## Schedule 2
## TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

### ALTERYX SECURITY STANDARDS

Alteryx abides by the security standards set out in this Schedule 2. Alteryx may update or modify these security standards from time to time, in its sole discretion, provided that such modifications will not result in a material degradation of the security of the relevant Licensed Products and any services (collectively, the "Services") during the term of the Agreement.

### 1. GENERAL PROVISIONS

**1.1 Data Neutral**. Alteryx is unaware of which data types its customers upload to and use with the Services and will process all data, regardless of its nature, as long as it fits the pre-defined characteristics that allow it to be processed as part of the Services.

**1.2 No Employee Interaction**. Alteryx employees do not directly interact with Licensee Content as part of their normal job duties except for the purpose of providing support services to customers upon request and as agreed in advance.

**1.3 Licensee Content**. Licensee Content is preserved in encrypted form using industry standard encryption, in customer-specific S3 buckets. Each Authorized User may delete the content they upload or link to the Services as part of the self-service options available within the Alteryx platform.

**1.4 Shared Responsibility.** Alteryx customers are strongly discouraged from sending highly sensitive data (such as PCI or ePHI) to the Services. Alteryx provides appropriate security for its Services but each customer must take care to use all Services responsibly and in accordance with any industry or professional standards applicable to such customer. Licensee must also maintain appropriate controls to secure Licensee's user accounts and credentials.

**1.5 Industry Requirements.** Licensee is responsible for understanding and applying any laws, regulations, or industry standards specific to Licensee's industry or Licensee Content.

**1.6 Definitions:**

1.6.1 Licensee – the entity that licenses relevant Alteryx Licensed Products pursuant to the Agreement

1.6.2 Licensee Content – Licensee's intellectual property, confidential information, and any Personal Data processed for or on behalf of the Licensee as part of the information uploaded or connected to the relevant Licensed Products by Licensee for Licensee's exclusive use

1.6.3 Personal Data – as defined by the DPA

1.6.4 Subprocessor- as defined by the DPA

## 2. INFORMATION SECURITY PROGRAM

**2.1 Information Security Program.** Alteryx maintains an information security program (the "**Program**") that utilizes policies, procedures, and standards to protect the confidentiality, integrity and availability of information and data, whether in electronic or tangible form. The Program is based on ISO/IEC 27001 and (i) defines, implements and includes periodic reviews of Alteryx's information security policies and procedures, including those for accessing and transmitting Licensee Content; (ii) is designed to prevent unauthorized access, acquisition, release, modification or use of Licensee Content; and (iii) is designed to protect against threats or hazards to the security or integrity of Licensee Content based on a current understanding of the security environment and evolving risk factors.

**2.2 Control Requirements.** Alteryx maintains adequate administrative, technical, and physical controls designed to safeguard Licensee Content in accordance with relevant privacy, data, and security regulations and laws ("**Security Standards**"). Alteryx's Security Standards consider the sensitivity of the Services and the risks that pertain to processing of Licensee Content as part of the Services and as contemplated by the Agreement.

2.2.1 User Access Management. Alteryx implements access control policies to support creation, amendment, and deletion of user accounts for systems or applications storing or allowing access to Licensee Content. Alteryx's user account and access provisioning process assigns and revokes access rights to systems and applications, restricting access to only those Alteryx personnel and Subprocessors that require access, and solely to the extent so required, to fulfill Alteryx's obligations under the Agreement or to comply with applicable law.

2.2.2 Secure User Authentication. Alteryx ensures proper user authentication for all of its personnel with access to Licensee Content, including by: assigning each employee unique access credentials for the system on which Licensee Content may be accessed and prohibiting employees from sharing their access credentials; and using access control lists and firewall rules. Alteryx ensures that all persons having access to Alteryx systems or any Licensee Content have appropriately controlled and limited access, access is removed or restricted when no longer required or appropriate, and access is promptly removed following termination.

2.2.3 Personnel Training and Background Checks. Alteryx provides annual security awareness and privacy training to all personnel who process or may have access to Licensee Content. Where permitted by law, Alteryx performs adequate background checks on all personnel who have access to Licensee Content.

2.2.4 Passwords and Multi-factor Authentication. Alteryx maintains industry standard password security for all employee accounts. Policies include minimum length, complexity, restrictions on password reuse, number of password resets in a given timeframe, and frequency in which passwords must be changed. Alteryx has implemented and maintains a multi-factor authentication method required for access to applications and systems containing or accessing Licensee Content.

2.2.5 Subprocessor Assessments. Prior to engaging new third-party Subprocessors that will have access to Licensee Content, Alteryx will conduct a risk assessment of the data security practices of such Subprocessors, as well as periodic reviews to ensure their data security practices continue to meet Alteryx's obligations under this Schedule 2 and, where applicable, the DPA.

**2.3 Data Security**

2.3.1 Encryption. Alteryx utilizes current encryption technology, including encryption protocols, file encryption and database encryption, to protect Licensee Content both in transit and at rest.

2.3.2 Vulnerability & Patch Management. Alteryx maintains a vulnerability management process to identity and remediate vulnerabilities by performing vulnerability scans, implementing vendor patches or fixes, and developing a remediation plan for critical vulnerabilities. Alteryx applies security patches on a regular basis to systems used to access or process Licensee Content.

2.3.3 Data Separation. Alteryx logically separates Licensee Content from all other Alteryx and third-party data.

2.3.4 Incident Response Plan. Alteryx maintains an incident response program to address any suspected unauthorized access to or use of Licensee Content or to Alteryx systems that process or have access to Licensee Content, including, but not limited to: (i) promptly notifying Licensee of a confirmed breach, together with sufficient detail to inform Licensee of any potential risks to Licensee systems or data; (ii) taking all reasonable steps required to address the source of the suspected breach and to mitigate any identified risks; and (iii) providing Licensee with updates and information to demonstrate adequate resolution of the vulnerabilities giving rise to the suspected breach.

2.3.5 Policies. Alteryx maintains policies and procedures to prevent the unauthorized disclosure or use of Licensee Content and ensures that Alteryx personnel attest to such policies and procedures upon hire and annually thereafter.

2.3.6 Alteryx limits access to Alteryx computers and networks that process or may access Licensee Content through the use of one or more of the following: (i) username & password; (ii) multi-factor authentication; (iii) access control lists; and (iv) firewall rules.

2.3.7 Alteryx maintains network devices and servers in data centers that employ industry-accepted procedures and tools, including, at a minimum: (i) restricting both physical and network access to those with a business need for access; (ii) restricting physical access to the data centers by card-key control systems; (iii) implementing a network-based intrusion detection and prevention system; (iv) implementing firewalls to segment networks; (v) implementing security vulnerability assessment processes and tools; (vi) implementing change management procedures; (vii) implementing patch management processes and tools; and (viii) periodically backing up data maintained on Alteryx network servers and encrypting back-up media for storage off-site.

**2.4 Application Security**

2.4.1 Change Control. Alteryx maintains policies and procedures for managing changes and updates to production systems, applications, and databases, including processes for documenting security patching, authentication, and the testing and approval of changes into production.

2.4.2 Key Management. Alteryx implements key management procedures that include the secure generation, distribution, activation, storage, recovery, and replacement of cryptographic keys. Keys are rotated on a regular basis and lost, corrupted, or expired keys are immediately revoked or disabled.

2.4.3 Logging**.** Alteryx logs security information from systems and applications that store, allow access to, or process Licensee Content. These logs capture key security event types upon the detection of suspicious system and/or user behaviors.

2.4.4 Intrusion Detection. Alteryx has implemented and maintains an intrusion detection monitoring process at the network and/or host level to detect unwanted or hostile network traffic. Alteryx will update its intrusion detection software regularly, on a scheduled basis following the availability of such updates by the software provider.

2.4.5 Secure Coding Practices. Alteryx logically or physically separates environments for development, testing, and production. Licensee Content is not used in development or testing environments.

**3. TESTING AND AUDITS**

**3.1 Penetration Tests**. At least once annually, Alteryx undertakes penetration testing of the Licensed Products by an independent third party and promptly remediates all critical and high vulnerabilities identified in penetration test results. All other findings are remediated in a timeframe that is commensurate with the identified risks.

**3.2 Compliance.** Alteryx shall either provide attestation statements and reports regarding its security certification programs (where applicable) or complete Licensee's security questionnaire, upon Licensee's reasonable, written request. Requests for reports or security questionnaires are permitted once per rolling calendar year, provided, however, that Licensee may request additional assurances in the event of a confirmed breach of Alteryx's systems used to process Licensee Content.

**3.3 Vulnerability Scanning.** Alteryx maintains a vulnerability management program and performs regular vulnerability scanning against services and key infrastructure utilizing industry standard tools or well-known external suppliers.

**4. DATA USE, RETENTION AND DELETION**

**4.1 Permitted Use**. Alteryx may only use Licensee Content as outlined by and for the duration of the Agreement. Licensee Content may not be shared with third parties except as permitted by the Agreement, including, where applicable, the terms of the DPA. Notwithstanding an obligation of Alteryx to retain certain, limited Licensee Content for the period designated by applicable law or regulation, Alteryx may only retain Licensee Content as expressly permitted by Licensee for the purpose of providing the Services.

**4.2 Secure Deletion**. Upon expiration or termination of the Agreement for any reason, Alteryx shall promptly delete or destroy all Licensee Content, taking into account currently available technology so that Licensee Content cannot be reasonably read or reconstructed, including by rendering unreadable any media on which Licensee Content is stored.

**4.3 Data Storage**. Unless otherwise expressly agreed in an Order Form, Alteryx stores Licensee Content in the United States and may process License Content in order to provide the Services in any country in which Alteryx operates.

**5. DISASTER RECOVERY & BUSINESS CONTINUITY**

**5.1** Alteryx maintains a disaster recovery/business continuity program that includes: (i) disaster recovery/business continuity plans and procedures; (ii) back-up recovery processes designed to ensure that critical business functions can be resumed within specified timeframes; and (iii) a process to regularly review, test and update the disaster recovery/business continuity program as needed.