

ALTERYX DATA PROCESSING AGREEMENT

This Alteryx Data Processing Agreement (“**DPA**”) is incorporated into and supplements the Agreement (as defined below) and solely applies to the processing of Customer Content by Alteryx and Alteryx’s Affiliates. In the event of a conflict between this DPA and any other documents that comprise the Agreement, this DPA controls with respect to Alteryx’s processing of Personal Data for or on behalf of Alteryx’s customers.

1. Definitions

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

Term	Definition
Agreement	The Alteryx End User License Agreement or the master agreement (e.g., Master License Agreement) between Alteryx and its customers (each, “ Customer ” or “ Licensee ”) governing the Services.
Applicable Law	The relevant data protection and data privacy laws, rules, and regulations directly applicable to this DPA, including, but not limited to, the General Data Protection Regulation (EU 2016/679) (“ GDPR ”) and the California Consumer Privacy Act and California Privacy Rights Act (“ CCPA/CPRA ”), and all other enacted state data protection and privacy laws (e.g., the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Data Privacy Act) and any successor laws, rules and regulations. For the avoidance of doubt, “Applicable Law” will include other state, federal, and international data protection and data privacy laws not expressly named above to the extent applicable to this DPA.
Cloud Content	Any data or information that a customer uploads, connects to, or imports into Alteryx cloud environments for use with the Services, from its internal data sets or other sources not supplied by Alteryx (e.g., Licensee-Sourced Data), together with any workflows, recipes, insights, output content, or other materials created by customer using the Services, and any log-in credentials for accessing or linking to third-party data sources while using the Services.
Customer Content	Collectively, Cloud Content and Services Content. For the avoidance of doubt, Customer Content is considered “Licensee-Sourced Data” or “Licensee Content” under the Agreement. Usage Data is expressly excluded from Customer Content.
Personal Data	Collectively referred to as “Personal Data” for the purposes of this DPA, encompasses “personal data”, “personally identifiable information”, or “personal information” as defined under Applicable Law.
“process”, “processes”, “processing” and “processed”	Any operation or set of operations 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.
SCCs	The Standard Contractual Clauses approved by the European Commission under Decision 2021/914 of 4 June 2021, as currently provided at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj , as may be modified or supplemented from time to time, or, as applicable, the United Kingdom’s International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0), in force 21 March 2022 (“UK SCCs”).
Security Incident	A breach of Alteryx security leading to the accidental or unauthorized destruction, loss, alteration, disclosure of, or access to Customer Content.
Services	All Alteryx cloud-based products, professional services, and support services provided to a customer pursuant to an Order Form.
Services Content	Services Content includes logs uploaded by the Customer related to a support request and any raw data provided or made accessible to Alteryx or its Subprocessors in providing professional services pursuant to an Order Form.
Subprocessor	Contractors, vendors, and third-party service providers engaged by Alteryx to process Customer Content on terms consistent with this DPA.
Usage Data	Data that Alteryx collects directly from users of its Services to monitor the performance of the Services, provide support and troubleshooting, verify authorized use of the Services for security and licensing purposes, and in aggregated and de-identified form, to improve the Services.

2. Obligations of the Parties

2.1. **Role of the Parties.** For purposes of this DPA, the parties may act in the following capacities:

Party	Role	Description of Role
Customer	Controller	Customer is deemed a controller if it determines the purposes and means of processing of Personal Data in Customer Content.
	Processor	To the extent a third party determines the purposes and means of Customer's processing of Personal Data in Customer Content, Customer's role will be a processor, provided that Customer will act in the capacity of a controller with respect to this DPA and any controller instructions provided to Alteryx hereunder.
Alteryx	Processor	Alteryx is acting in the capacity of a processor or subprocessor, as applicable, on behalf of Customer with respect to Customer Content.

The terms "controller", "processor", and "subprocessor" have the meanings set forth in the GDPR (or equivalently defined terms under other Applicable Laws).

2.2. **General Compliance.**

- a. Alteryx will process Customer Content in compliance with this DPA and Applicable Law.
- b. Customer will comply with its obligations as a controller or processor with respect to this DPA and Applicable Law. If Customer processes Customer Content on behalf of a third party, Customer is solely responsible for ensuring that use of the Services and any instructions provided to Alteryx pursuant to this DPA comply with all instructions of such third-party controller.

2.3. **CCPA/CPRA.** The Parties acknowledge that Alteryx is a "**Service Provider**" (as defined by CCPA/CPRA) with respect to the processing of Customer Content under this DPA. Alteryx does not provide Customer with monetary or other valuable consideration in exchange for any Personal Data contained within Customer Content. Except as required by applicable law or regulation, Alteryx will not collect, access, use, disclose, process, or retain Personal Data contained in Customer Content for any purpose other than providing the Services or another business purpose expressly permitted by CCPA/CPRA (including 11 CCR § 7051(c)), this DPA, or the Agreement. Alteryx further acknowledges that, with respect to Personal Data in Customer Content that Alteryx processes as a Service Provider on behalf of Customer subject to both this DPA and CCPA/CPRA, or as otherwise required by the Applicable Law of other states:

- a. Alteryx is obligated to comply with and provide the same level of privacy protection as required by Applicable Law.
- b. Customer may take reasonable and appropriate steps to ensure that Alteryx uses such Customer Content in a manner consistent with Customer's obligations under Applicable Law.
- c. Alteryx must notify the Customer if Alteryx determines that it can no longer meet its obligations under Applicable Law, and upon such notice, grant Customer the right to take reasonable and appropriate steps to stop and remediate unauthorized use of such Customer Content, as otherwise outlined by this DPA or expressly proscribed by Applicable Law.
- d. Alteryx is prohibited from combining such Customer Content that it receives from, or on behalf of, the Customer with Personal Data that it receives from, or on behalf of, another person or persons (or a CCPA/CPRA household), or collects from its own interaction with a person or persons (or a CCPA/CPRA household), provided that Alteryx may combine personal information to perform the Services.
- e. Alteryx will not sell or share (as "sell" and "share" are defined and governed by Applicable Law, including CCPA/CPRA) any Personal Data subject to this DPA.

2.4. **Controller Instructions.** Alteryx will process Customer Content in accordance with Applicable Law and Customer's written instructions and as outlined in [Schedule 1](#) and any Customer configuration of the Services. Customer acknowledges and agrees that it is solely responsible for understanding and applying

any laws, regulations, or standards specific to Customer's industry or Customer Content. This DPA and the Agreement, together with any Customer configuration of the Services, set out Customer's complete instructions regarding Alteryx's processing of Customer Content. Additional instructions (if any), other than a written instruction from Customer to Alteryx to suspend or stop processing Customer Content, will require a prior, written amendment to this DPA.

- 2.5. **Customer Contacts.** For Customer and those entities that Customer permits to use the Services, Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Customer Content in accordance with this DPA, including, if applicable, Customer's use of Alteryx as a processor or subprocessor hereunder. When Alteryx informs or gives notice to Customer under this DPA, such information or notice is deemed received by those entities permitted by Customer to use the Services and it is Customer's responsibility to forward such information or notices to such entities.
- 2.6. **Data Subject Requests.** If a data subject makes a request to Alteryx with respect to Personal Data contained within Customer Content and identifies Customer as the controller of such Personal Data, Alteryx will promptly inform and reasonably cooperate with Customer regarding such request, as required by Applicable Law, and Customer will be solely responsible for responding to the data subject and taking such additional steps as are required to satisfy the request. Customer acknowledges that the Services do not include the right of Alteryx to access Cloud Content in a manner necessary to determine whether specific Personal Data exists in such Cloud Content, or to verify a data subject request and take action with respect to a specific individual whose Personal Data may be included in Cloud Content.
- 2.7. **Agreement Limitations Apply.** To the maximum extent permitted by Applicable Law, including Clause 12 of the SCCs (Liability), any claims brought under or in connection with this DPA, including any claims brought by those entities that Customer authorizes to use the Services pursuant to the Agreement, will be subject to the exclusions and limitations set forth in the Agreement.
- 2.8. **No Third-Party Beneficiaries.** Except as expressly required by Applicable Law, including Clause 3 of the SCCs (Third Party Beneficiaries), no one other than a party to this DPA, its successors and permitted assigns has any rights under this DPA or may enforce its terms.
- 2.9. **Usage Data.** Consistent with common software industry practices, Alteryx collects Usage Data directly from users of its Services in the ordinary course of its business and for Alteryx's internal business operations. To the limited extent that Usage Data may contain Personal Data, Alteryx collects such data directly from its users as an independent controller in accordance with Alteryx's Privacy Policy found at <https://www.alteryx.com/privacy>, and consistent with its obligations under relevant privacy laws globally. Where feasible, Usage Data is de-identified prior to use by Alteryx except when use in unredacted form pertains to Alteryx's provision of products and Services to the user or Customer, such as for license compliance and security-related purposes. Usage Data does not include Customer Content, nor any Personal Data included in Customer Content.

3. Subprocessors

- 3.1. **Subprocessor Changes.** Alteryx's list of Subprocessors for Customer Content can be found at <https://www.alteryx.com/subprocessors>. This list will be updated at least thirty (30) days in advance of any intended Subprocessor changes. To receive notice of such changes via email, Customer must subscribe to Subprocessor updates. If Customer does not subscribe to email updates, Alteryx's posting of the updated Subprocessor list on its website will be deemed to constitute notice to Customer in accordance with this provision. Customer will have fifteen (15) calendar days following provision of notice in accordance with this Section 3.1 to object in writing to a new Subprocessor of Customer Content. In the event Customer objects within such 15-day period, Alteryx will make commercially reasonable efforts to address Customer's good faith objection based on data privacy concerns, or, where feasible, to suggest a commercially reasonable change to Customer's configuration of the Services to

avoid processing of Customer Content by the objected-to Subprocessor. With respect to the GDPR, SCC Clause 9(a), Option 2 (General Written Authorization), governs Alteryx’s use of Subprocessors of Customer Content to deliver the Services.

3.2. Subprocessor Security

- a. Alteryx will perform appropriate due diligence, including security reviews, of all Subprocessors prior to engagement to process Customer Content. Subprocessors will be assessed annually to validate each Subprocessor’s material compliance with Alteryx’s stated privacy and security obligations.
- b. Alteryx will contractually bind all Subprocessors to terms no less stringent than those applicable to Alteryx under this DPA to the extent of the services performed by the Subprocessor.
- c. Alteryx is responsible for the performance of obligations by a Subprocessor to the same extent such obligations were directly performed by Alteryx under this DPA, and Alteryx will remain liable for the acts and omissions of its Subprocessors with respect to the processing of Customer Content.

4. SCCs and International Transfers

- 4.1. **Processing Locations.** Alteryx may transfer and process Customer Content, including any Personal Data, in the United States and in other locations throughout the world where Alteryx, its Affiliates or its Subprocessors maintain data processing operations, provided that such processing complies with the requirements of this DPA and Applicable Law.
- 4.2. **Transfers from the EEA.** To the extent that Personal Data under this DPA is transferred by or on behalf of Customer from within the European Economic Area (EEA) to Alteryx in a jurisdiction outside of the EEA, and to the extent such transfer is restricted under the GDPR, the Parties agree that the SCCs will provide the appropriate transfer safeguards, subject to the following modifications:

SCC Reference	Title	Application
Module Two and Module Three	<u>Module Two</u> : Controller to Processor <u>Module Three</u> : Processor to Processor	Module Two or Module Three will apply, depending on whether Customer is a controller or processor of the Customer Content. In each case, Alteryx is a processor to Customer.
Clause 7	Docking Clause	The optional docking clause will apply.
Clause 9(a), Option 2	Use of Subprocessors	General Written Authorization will be used for Subprocessors, as described in Section 3.1 above.
Clause 11	Redress	The optional language regarding independent dispute resolution will not apply.
Clause 17, Option 1	Governing Law	The SCCs will be governed by the laws of Germany.
Clause 18(b)	Forum and Jurisdiction	All disputes will be resolved before the courts of Germany.
Annex I	List of Parties, Description of Transfer and Competent Supervisory Authority	<u>Annex I</u> is deemed completed with the information set out in Schedule 1 to this DPA.
Annex II	Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data	<u>Annex II</u> is deemed completed with the information set out in Schedule 2 to this DPA.
Annex III	List of Subprocessors	<u>Annex III</u> is deemed completed using the Subprocessor List found at https://www.alteryx.com/subprocessors .

4.3. **Transfers from the United Kingdom, Switzerland, or Brazil.** To the extent that Personal Data under this DPA is transferred by or on behalf of Customer from within the United Kingdom, Switzerland, or Brazil (each a “Restrictive Jurisdiction”) to Alteryx in a different jurisdiction, and to the extent such transfer is restricted under Applicable Law, then the SCCs, as modified above, provide the appropriate safeguards required of such a transfer, subject to the following additional modifications:

a. **References Modified.**

SCC References	Modification to the SCC References
“Regulation (EU) 2016/679”, “the Regulation”, or the GDPR	Will be interpreted as references to the Applicable Law of the Restrictive Jurisdiction.
Articles of the GDPR	Where required or appropriate, references to specific Articles will be replaced with the equivalent article or section of the Applicable Law of the Restrictive Jurisdiction.
“EU”, “Union” and “Member State”	Will be replaced with references to the Restrictive Jurisdiction.
“Competent supervisory authority”	Will be the UK Information Commissioner, the Swiss Federal Data Protection and Information Commissioner, or Brazil’s National Data Protection Authority, as applicable.
“Competent courts”	Will mean the courts of England and Wales, Switzerland, or Brazil, as applicable.

- b. **Governing Laws; Forum and Jurisdiction.** In Clause 17 and Clause 18(b), the SCCs will be governed by the laws of United Kingdom (England and Wales), Switzerland, or Brazil, as applicable, and disputes will be resolved before the courts of the United Kingdom (England and Wales), Switzerland, or Brazil, as applicable.
- c. **The United Kingdom’s Addendum.** The United Kingdom’s International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0), in force 21 March 2022 (the “UK Addendum”) is attached to this DPA as [Schedule 3](#).

5. Information Security Program

- 5.1. **Technical and Organizational Measures.** Alteryx maintains appropriate technical and organizational measures designed to protect Personal Data as required by Applicable Law (the “Information Security Program”) and as identified in [Schedule 2](#). Alteryx will regularly monitor the effectiveness of its Information Security Program and implement additional security measures as reasonably appropriate to maintain the security of the Services with respect to Alteryx customers and Customer Content generally.
- 5.2. **Program Updates.** Customer 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 Services.
- 5.3. **Customer Use of Services.** Except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Content when in Customer’s possession or control, and ensuring the secure transmission of Customer Content to and from the Services to the extent such transmission is not in Alteryx’s control. It remains Customer’s responsibility to (a) retain or backup any Customer Content it uploads to the Services, and (b) secure any Customer environments from which Customer Content is processed as part of the Services.

6. Audits

- 6.1. **Security Questionnaires.** Customer may reasonably request that Alteryx provide assurance of Alteryx’s compliance with its obligations to Customer hereunder upon at least thirty (30) days’ prior written notice through the submission of security questionnaires or a request for the most recent, relevant

third-party certifications or summary executive findings pertaining to Alteryx's Information Security Program. Notwithstanding any requests made by data protection authorities or as otherwise required by Applicable Law, Customer may make a request under this Section 6.1 no more than once per rolling calendar year. In lieu of providing responses to customer-specific security questionnaires, Alteryx may provide industry accepted security questionnaire responses, such as CSA Consensus Assessment Initiative Questionnaires responses (CAIQs) or Security Information Gathering Questionnaire responses (SIGs). If these industry accepted security questionnaire responses do not adequately address substantive questions included in a customer-specific security questionnaire, Alteryx will provide commercially reasonable assistance to Customer in providing appropriate responses to those questions.

- 6.2. **Audits.** To the extent expressly permitted by the SCCs or Applicable Law, Customer may, at Customer's expense, request reasonable supplementary information through an audit of the Information Security Program and Alteryx's policies and procedures related to this DPA. Any such audit may be conducted by Customer or a mutually acceptable third-party auditor subject to an Alteryx non-disclosure agreement. The parties will reasonably cooperate and agree in advance as to the time, manner, and scope of this audit. The audit will be conducted remotely unless the parties mutually agree in writing, signed by an authorized representative of each party holding the title of vice-president or above, that the purposes of this Section 6.2 cannot be reasonably accomplished without an on-site audit. Any necessary on-site audit activities will be conducted after the remote audit is completed, at which time the parties will agree to the remaining audit activities, which will be limited to only those remaining activities necessary to reasonably accomplish the audit purposes. Notwithstanding any requests made by data protection authorities or as otherwise required by Applicable Law, Customer may make an audit request under this Section 6.2 no more than once per rolling calendar year.

7. Cooperation

- 7.1. Taking into account the nature of processing and information available to Alteryx, Alteryx will reasonably cooperate with Customer as necessary:
- for Customer to comply with its obligations under Applicable Law, or
 - to address Customer's concerns if Customer has a reasonable and good faith belief that Alteryx's processing of Customer Content does not comply with Applicable Law.

In each case, Customer must provide reasonably sufficient details to Alteryx as needed to understand the basis for Customer's requests or concerns.

8. Deletion of Customer Content and Termination

- 8.1. **Data Deletion.** Alteryx will promptly and securely delete Customer Content after expiration or termination of the Agreement and otherwise in accordance with Applicable Law. Alteryx may provide Customer with self-service functionality that enables Customer to (a) download or export and retain Cloud Content for itself if Customer chooses, and (b) delete Cloud Content prior to expiration or termination of the Agreement. Customer must take the steps available through this self-service functionality to delete Cloud Content prior expiration or termination of the Agreement. Customer may request reasonable assistance with respect to retention or deletion of Cloud Content prior to the date of expiration or termination by opening a support request with Alteryx. Any remaining Cloud Content that Customer does not delete prior to expiration or termination of the Agreement will be deleted by Alteryx in accordance with the time periods set out in Alteryx's internal retention schedules and, where applicable, the requirements of Applicable Law.
- 8.2. **Data Transfer Option.** Where expressly designated in an Order Form, Alteryx may provide Customer a limited, specified period following termination or expiration (not to exceed 30 calendar days) during which Customer may use self-service tools to back-up or export Cloud Content from Alteryx cloud-based

products. Notwithstanding the foregoing, following any such specified period of retention for Customer's benefit, Alteryx will have no obligation to retain Cloud Content.

- 8.3. **Termination.** This DPA terminates simultaneously and automatically with deletion of all Customer Content following termination or expiration of the Agreement.

9. Security Incidents

- 9.1. **Security Incident Procedures.** Alteryx will implement and maintain policies and standards to (a) identify, detect and respond to suspected or known Security Incidents, mitigate harmful effects of Security Incidents, and document Security Incidents and their outcomes, and (b) restore the availability or access to Customer Content in a timely manner.
- 9.2. **Notice.** Alteryx will provide prompt written notice (email will suffice) to Customer, without undue delay and where feasible, once Alteryx becomes aware that a Security Incident has taken place, except to the extent such notice is restricted by law enforcement or may permit exploitation of the Security Incident. To the extent known by Alteryx, such notice will include all available details required under Applicable Law to enable Customer to comply with its notification obligations to regulatory authorities or individuals affected by the Security Incident, including a description of the Security Incident, the types of data or number of users whose Personal Data may be impacted, and the remediation efforts taken or planned. If and to the extent Alteryx confirms that a Security Incident impacts Personal Data included in Customer Content, Alteryx will provide notices required by this Section 9.2 in the time and manner required by Applicable Law and the SCCs. Alteryx shall take commercially reasonable steps to investigate, contain and remedy the Security Incident and to prevent any further such incidents.

10. Compelled Disclosures

- 10.1. If Alteryx is ordered or otherwise compelled to provide any Customer Content to any law enforcement or other government agency (an "Authority"), Alteryx shall:
- a. Request that the Authority direct its order to Customer and not Alteryx;
 - b. Notify Customer of the order, unless Alteryx reasonably understands that it is prohibited by law or by the Authority to notify Customer, in which case Alteryx will use commercially reasonable and lawful efforts to have the Authority permit Alteryx's notification to Customer; and
 - c. Assist Customer, at Customer's expense, to lawfully challenge the order to the extent such challenge can be validly raised pursuant to the applicable jurisdiction and laws under which the order was made.

SCHEDULE 1 (Annex I to the SCCs)

A. LIST OF PARTIES

Data exporter(s):

Name: Customer, as named in the Agreement, and those Customer Affiliate(s) authorized to purchase products and services from Alteryx as expressly identified 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 Customer Content with the Services for Customer's benefit or the benefit of Customer's employees, customers, and partners.

Role (controller/processor): controller, or a processor on behalf of a third party.

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 Customer Content, which may, in Customer's sole discretion, include Personal Data

Role (controller/processor): processor on behalf of Customer

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Solely determined by Customer as part of Customer Content.

Categories of personal data transferred

Solely determined by Customer as part of Customer 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.

Any use of the Services with Customer Content that contains sensitive data is at Customer's sole discretion, in accordance with Schedule 2.

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

Frequency of transfers of Customer Content that include Personal Data are at Customer's sole discretion in its use of the Services.

Nature of the processing

Hosting of Customer Content, which may contain Personal Data, for Customer's use of the Services.

Purpose(s) of the data transfer and further processing

Personal Data may be transferred as part of Customer Content solely for Customer's use of the Services 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

Customer is solely responsible for determining the retention period of any Customer Content, including Personal Data, during the term of the Agreement.

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

Subprocessors engaged to process Customer Content are as outlined at <https://www.alteryx.com/subprocessors>.

C. COMPETENT SUPERVISORY AUTHORITY

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

Bavarian State Office for Data Protection Supervision

SCHEDULE 2 (Annex II to the SCCs)

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Alteryx's Information Security Program Description that details Alteryx's technical and organizational measures is incorporated by reference into this Schedule 2 and is located at: <https://www.alteryx.com/security-standards>.

SCHEDULE 3 – UK Addendum

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		
Start date	The effective date set forth in the Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: See Agreement Trading name (if different): See Agreement Main address (if a company registered address): See Agreement Official registration number (if any) (company number or similar identifier): See Agreement	Full legal name: Alteryx, Inc. Main address (if a company registered address): 17200 Laguna Canyon Rd, Irvine, CA 92618 USA Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): See Agreement Job Title: See Agreement Contact details including email: See Agreement	Full Name (optional): Jennifer Sivan Davide Job Title: Senior Director, Privacy and Product Counsel and Data Protection Officer Contact details including email: jennifer.davide@alteryx.com
Signature (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses	
Addendum EU SCCs	<input checked="" type="checkbox"/> The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No	N/A	N/A			
2	Yes	Yes	No	General	30	
3	Yes	Yes	No	General	30	
4	No	N/A	N/A			N/A

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: [Schedule 1.A](#) of this DPA

Annex 1B: Description of Transfer: [Schedule 1.B](#) of this DPA

Annex II: Technical and organisational measures to ensure the security of the data: [Schedule 2](#) of this DPA

Annex III: List of Sub processors (Modules 2 and 3 only): www.alteryx.com/subprocessors

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

Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 of those Mandatory Clauses.