



How Alteryx Uses Data

Like any company, data and information comes to Alteryx from different sources and for different purposes. The ultimate goal of interacting with this data is to help our customers and the broader Alteryx community create breakthrough outcomes with analytics automation (click [here](#) about “Why Alteryx”). We know that to fully enable your use [Alteryx’s software and cloud services](#) (our “products”), as well as our [Community](#) and [websites](#), you will want to understand how we use data.

Our Guiding Principles

The principles that guide Alteryx’s culture of respect, transparency, and inclusion also guide our collection and use of data:

- Customer First** We believe customers should decide what happens to the data they upload into our platforms.
- Integrity** We are transparent about how we use your data.
- Accountability** We take appropriate measures to secure the data entrusted to us. When it comes to personal data, we respect an individual’s privacy and only collect, use and share personal data according to applicable privacy laws.
- Equality** We respect the data received from all sources, including our customers and community of Alteryx users.
- Empowerment** We let customers and users control the personal data they each provide us.

Cloud Content

When a customer uploads, connects to, or imports data into our cloud products, including the [Alteryx Analytic Cloud Platform](#) and other Alteryx applications, we understand and appreciate that the data is there for the customer’s use and nothing else. This data, along with workflows, log-in credentials and the results of your work while using our cloud products is what we refer to as “**Cloud Content.**”

We don’t use your Cloud Content

Simply put, we don’t use your Cloud Content. You upload or connect Cloud Content to our products so you can interact with the data, build workflows, and find answers and insights. We simply provide you with the software tools to accomplish that task.

We don’t access your Cloud Content

Since we don’t have a need to use or interact with your Cloud Content, we don’t access that data, except for the very limited circumstances described below for our cloud products. Our cloud platform runs entirely in trusted third-party cloud services such as AWS and Google Cloud, which logically and physically separates our network and systems that our personnel use from the platform that processes Customer Content. This, together with the fact our personnel don’t need to interact with Customer Content, allows us to strictly limit our personnel’s access rights to this platform. The only reason our personnel are granted access is for limited administration and security purposes, or to respond to your

support requests in which you specifically ask us to access the cloud environment. In these events, we strictly limit that access for only a limited time and access is monitored and logged.

What about Personal Data in Customer Content?

Our customers control what's included in their Customer Content. Given the access limitations described above, we won't know what you decide to include in Customer Content. Nevertheless, we operate with the assumption that Customer Content *may* contain personal data, and based on that assumption, we apply all applicable privacy laws to Customer Content in accordance with our [Data Processing Agreement](#).

Where is Customer Content stored?

Where Customer Content is stored is your choice. Our products can connect to your data sources using our secure [Data Connectors](#). Data uploaded and stored into cloud platform workspaces, including workflows and sample data, can be stored directly by Alteryx using a dedicated workspace such as an AWS S3 bucket or can be secured and stored directly in your own virtual private cloud environment using our Private Data Handling configurations. For more information about this option, please see our [Private Data Handling Whitepaper](#).

We don't receive or have access to Cloud Content from our On-Premises Products

When you use our on-premises products, the data you connect to use with our products remains with you. We don't receive or have access to your content from our on-premises products. As described below, the only data we'll receive is limited Services Content and Usage Data.

Services Content

If you need help from our customer support team, we're there to help. We use a "follow-the-sun" support model to help address your needs whenever and wherever needed. You choose what information to attach to a support case, which will mostly be crash logs. This data is what we refer to as "**Services Content**." After support case closure, and after a period of time in which we're reasonably certain that the case won't be re-opened for further support, we'll delete the Services Content associated to the case.

Services Content may contain a limited amount of personal data, such as the user's email address, IP address and similar. Here too, we comply with all applicable privacy laws as stated in our [Data Processing Agreement](#).

Personal Data collected directly from Users

Alteryx interacts with individual users of our products in various ways, including the [Alteryx Community](#), [Alteryx Certifications](#), [SparkED Education](#) and, of course, using our software and cloud products. For instance, when a user registers with us for these services, any personal information provided is collected and processed subject to Alteryx's [Privacy Policy](#).

Do we sell Personal Data?

No, we do not sell personal data. Privacy laws like the California Consumer Privacy Act also refer to “sharing” information, which we don’t do as well. In short, Alteryx’s foundation of respect, transparency and inclusion, and the associated principles described above, applies to our treatment an individual’s personal data as well as the data we receive directly from our customers.

Usage Data

“**Usage Data**” is telemetry and metadata *about our products* that we use to monitor product performance, help us pinpoint the sources or causes of product-related issues when providing support and troubleshooting, and to ensure compliance with our agreements and terms of use. We also use the learnings from Usage Data to improve user experiences with our products. For this particular purpose, we only use aggregated data that does not identify the users or any of our customers. Usage Data does not include Customer Content or Services Content.

Examples of Usage Data

Examples of Usage Data include:

- Usage details relevant to troubleshooting and error resolution, as well as to identify preventative support measures, such as software version number.
- How and when product features are used.
- Device data, such as number of cores.
- Browser interactions with the product, such as mouse clicks.
- Relevant product configurations, such as language preferences.

Personal Data in Usage Data

When personal data is included in Usage Data, it is very limited and directly relates to product information about the user’s interactions. As described above, this personal data is collected subject to Alteryx’s [Privacy Policy](#). Since Usage Data may be used to improve our products, all such data aggregated and de-identified before any such use.

Usage Data that identifies or could lead to the identity of an individual user is personal data and cannot be shared with customers unless Alteryx has a right and legitimate interest to share that information. Any non-personal Usage Data that may be shared with customers can be accessed by customers from Alteryx’s [License and Downloads Portal](#).

Review of Our Collection Practices

We regularly review our data collection practices to verify that we are complying with applicable laws and only collecting what we need based on our objectives for collection and the guiding principles described above. Access to Usage Data is limited to pre-approved use cases and only access to the required data for each specific use case is granted.

How Alteryx Protects Data

Alteryx has taken several steps to ensure that we treat all data entrusted to us accordingly. Alteryx has implemented policies, standards and procedures designed to maintain the confidentiality, integrity and availability of the information entrusted to us. Alteryx personnel are bound to a confidentiality commitment and a [Code of Business Conduct and Ethics](#). We also provide personnel with regular training and awareness regarding the handling of confidential information and personal data.

Alteryx has independently verified the adequacy of its information security management practices through an [ISO 27001 Certification](#) and a SOC2 Type 2 Audit. Please visit our [Trust site](#) for more information about our privacy and security practices.