TECHNICAL OVERVIEW:

Data Compliance with Data Dynamics

Literally every second of every day, **you generate data.** Loads and loads of data, in fact, in a wide number of forms and formats, ranging from the basic personal data you entered on a Website to win a contest to the driver's license you had to scan to rent a car to medical scans uploaded by your doctor. You generate data even when you don't realize you're generating data, just binge-watching your favorite show or idly looking at your phone.

Imagine that data that you generate multiplied by millions and millions of people around the world, and it becomes easier to understand the staggering growth of data globally. Current estimates put the total at 120 zettabytes, but many analysts believe it to be even higher.

Along with this growth has come an increasing call from users to **safeguard that data.** Users now are much more aware of how their personal information is being used, both by companies and bad actors, and they are demanding that information only be used with their **explicit consent.**

Because of this, governments worldwide have stepped in to set rules in place for the usage of consumer data, and with a global economy, and enterprise that wants to do business in those countries and regions **must comply with those rules.**

StorageX, Insight AnalytiX, and ControlX all work hand-in-hand to help ensure that **data compliance,** with functionality that covers multiple areas:

1 Data Discovery

How can you comply with data protection regulations if you don't know what data you even have? Scan your storage environment using StorageX to get detailed information about the data your enterprise handles and where it's located.

2 Data Tagging

While scanning your storage environment, you can tag your files and folders to better categorize your data. You can then use those tags later on to analyze or move those files and folders.

3 Data Mapping

Once you know where your data lives, use Insight AnalytiX to scan what is contained in that data to identify potential personal data that needs to be protected.

4 Data Classification

Different types of data need to be handled in different ways. Use standard templates built into Insight AnalytiX to classify data based on governmental and international regulatory guidelines.

5 Audit Logging

One of the things consumers most want to know is who is accessing their data and when. ControlX leverages blockchain technology to create immutable audit logs that track all data access.

Discovering Your Customers' Data

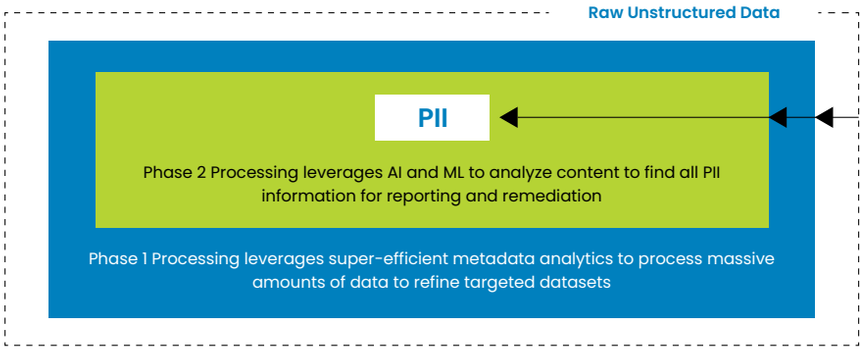
The initial step in the **data compliance** workflow must be to discover what data your enterprise actually has stored. You can take this **discovery** step using the StorageX Management Portal, which allows you to scan your storage environment and gather metadata about all of your files and folders.

This file and folder metadata is what we call **Phase 1 Processing,** where StorageX uses its own built-in metadata analytics to collect and sort your file-based data.

Tagging Your Customers' Data

When you run a scan on your storage resources, you can configure StorageX to assign a **custom tag** to the metadata for the files and folders it finds. This tag can allow you to more easily group or sort your files, both for analysis purposes and to potentially archive, migrate, or copy the files.

For example, if you create a scan in the **StorageX Management Portal** that includes only servers and filers in your company's European offices, you could set the scan to assign the tag **region,** with the value **europe.** You can then analyze only file metadata from those specific servers and filers by creating an analysis set that looks for the europe value for the region tag.



Mapping and Classifying Your Customers' Data

Sometimes it's not enough to know about the files themselves. When you need to ensure your enterprise complies with privacy or data-protection regulations, you need to know **what's inside those files.** That's where **Insight AnalytiX** comes into the workflow – Insight AnalytiX uses a dedicated machine learning model to search the content of **200+ different types of files**, looking for whatever type of data you want to find, from private medical information to vehicle identification numbers.

By default, Insight AnalytiX comes with several **pre-built templates** focusing on different areas, from financial information to healthcare-related information to human resources information. You can also create your own custom templates to better classify your sensitive data.

Insight AnalytiX does not store the potentially-sensitive information it finds, but instead **notifies you of the presence** of that type of information in each file. This type of data processing is what we call **Phase 2 Processing.** You can then run an **Entity Location Details Report** to find the specific line in each file where that information is located, all without actually exposing the data itself.

From there, you can evaluate what you need to do next to **remediate** any potential data compliance issues using ControlX or StorageX. You may opt to **quarantine** the sensitive data on a more protected server, to **secure** the data by modifying the ACLs on the affected files, or to track access to the files using an **audit trail.**

Auditing Access to Your Customers' Data

As mentioned above, one of the options for remediating potential data compliance issues using the Data Dynamics suite of products is to use ControlX to **create an immutable audit trail** for the files where Insight AnalytiX has found sensitive data.

In some situations, you may not be able to move or lock down files that contain personal or otherwise sensitive data. Instead, you can **monitor all access** to those files using the **blockchain** functionality built into ControlX. Any time a user touches one of the files, ControlX records that action in the file blockchain, which cannot be deleted or otherwise modified except by ControlX.

You can then use that blockchain, if necessary, to get the full, accurate history of all changes or access to a specific file in your environment. This allows you to better secure your customers' data and plug any holes or security breaches in your system.