Data Privacy Day: Take Stock of Your Data Retention and Deletion Policies

Today is Data Privacy Day—an annual reminder to brush up on and fine-tune our privacy and compliance best practices. It's also a great time to share the strides we've made, including Pure's recent ISO 27001 Certification, which demonstrates our commitment to keeping customers' data safe.

Compliance is a huge part of the privacy conversation, and it's a complex, ever-changing requirement. There's a critical aspect of compliance that's often overlooked, and it's nearly as important as how a customer's data gets used: **data retention and deletion policies.**

Last year, a €14.5 million GDPR fine was issued for a non-compliant retention schedule. And a report from 451 Research reveals that 31% of respondents aren't always following their deletion and retention policies—or haven't implemented retention policies at all.

If you have a retention and deletion schedule, it's critical that you're following it. If you don't, here's what you need to know—but note, this isn't legal advice and you should consult with your organization's lawyer or legal team.

What Is a Data Retention Schedule?

Data retention and deletion schedules address what happens to data after it's been used, dictating how long it can be stored and how it's disposed of. Even if you're not misusing the data and it's properly secured, retaining it beyond the cut-off date counts as an infraction.

A data retention schedule can be absolutely critical to this aspect of compliance. A retention and deletion policy will cover:

- What data sets you can store or archive
- Where these data sets can be stored (e.g., a data-only bunker)
- How long you can retain a data set in storage
- When a data set should be deleted or where it can be moved

In storing different data sets, I find one of the most helpful approaches is a tiered backup architecture. It allows you to separate snapshots that are hot, warm, or cold. A data-only bunker can safely store large amounts that aren't needed for immediate use. Check out this post for an example of a tiered bunker architecture you can create with Pure.

Note: You can set the schedules for retention and deletion, but they must be justified. You must provide adequate reasoning for the schedule and proof you're following it.

Why Have a Data Retention Policy?

One of the biggest compliance missteps I've seen companies make is keeping too much for too long. In many cases, keeping too much for too long can expose an organization to unnecessary risk. It's a bright, flashing target for bad actors and compliance officers alike. Not to mention, it can open your organization up to tremendous legal exposure.

General Data Protection Regulation (GDPR) calls this an individual's "**right to be forgotten**," and it essentially means a company can't hang on to their data when it's no longer needed for processing. But other regulations, like HIPAA and ISO, can contribute to what should be in your policy, so don't just stop at GDPR and consult your privacy expert.

The reason for this is that data sitting in archives or graveyards presents more risk for security breaches. If it's not needed and can be removed, your risk can be substantially lessened.

How to Create (or Improve) a Retention Schedule

First, know that your retention policy should be an integral part of your overall data security strategy. The two are inextricably linked. Start with a security review so that you can align the two. Then, create flow map for your organization. Your retention strategy should address data along the flow map, documenting exactly:

- What types are being stored and where—so it can be easily located when it's time to delete. This includes all traces, such as in backups or file servers.
- A permission-based framework for all retained data
- Anonymization and encryption policies that will be used
- How it's being processed and why
- Why it's being stored—including if there are legal or regulatory reasons for doing so, such as

audits or tax reasons, historic or research purposes, etc.
- When it's being deleted (or moved) and protocols for deletion or sanitization
- How you'll document deletion or anonymization
- Roles and responsibilities of individuals monitoring compliance and retention

Note: Sensitive personal information can be anonymized, which may preclude your need for retention or deletion of that particular set. However, if this data paired with another set can make it identifiable, it will still need to be deleted.

How Pure Storage Can Help Support Data Retention Strategies

Coupled with comprehensive organizational security measures, Pure Storage® can help you meet GDPR and other security requirements and data compliance regulations around the world, without adding more complexity.

- **The creation of tiered retained data with secure bunkers:** Given that communication is established into, but not out of, the bunker, it's considered a highly secure location.
- **Cloud-ready, seamless mobility:** Seamlessly move workloads to support changing business needs, including sets that no longer have value for processing.
- **Data and backups safe from encryption or deletion:** SafeMode™ snapshots protect your data, especially critical backups, from accidental deletion, compromised credentials, or encryption during an attack.
- **Modern protection:** We deliver the most modern data protection solutions, with security and rapid recovery against ransomware threats.
- **A single control pane for visibility:** It's important to have a clear handle on where your most important data lives at any given time. Pure's simple setup, effortless operations, and unified control pane make it easy to see what workloads are where, so you can move sets for deletion.

Your first step is to meet with your compliance officer and include your CISO to make sure everyone's on the same page.

Download the "FlashArray™ Data Security and Compliance" white paper for an in-depth look at how Pure can help your organization.