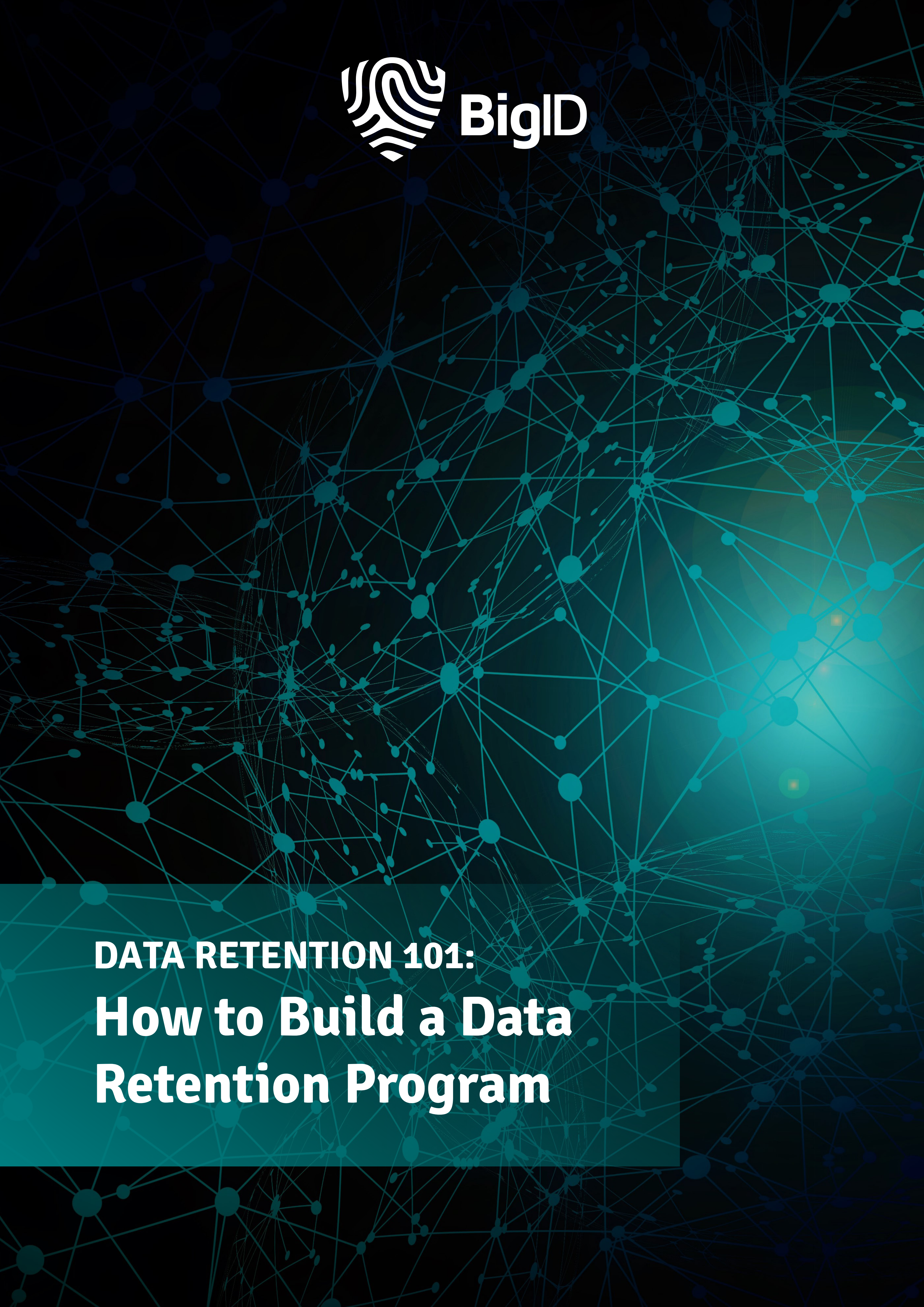
BigID



DATA RETENTION 101:

How to Build a Data Retention Program

Data retention is complex, nuanced, and requires a modern approach in order to handle the growing volume, type, and sensitivity of enterprise data. Organizations need help to define and manage data retention policies and remediate violations. They need to be able to operationalize a complex set of business rules and local and global regulations.

Many companies systematically over-retain data, opening them up to enormous risk. Around a third of data stores have not been touched for three years — and 75% of over-retained records include personal or sensitive data.

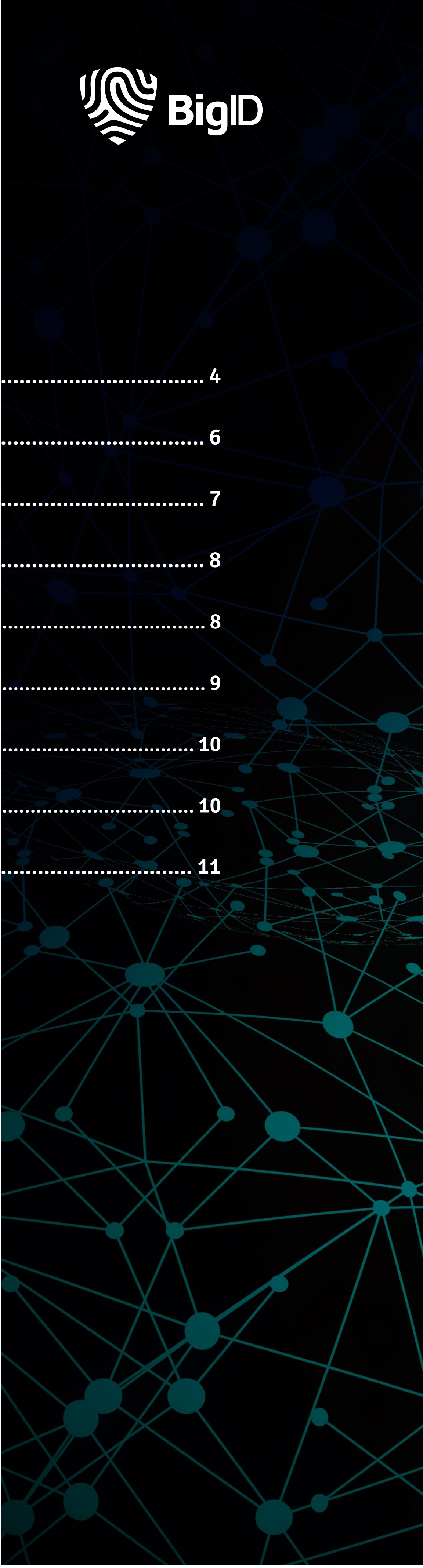


Table of contents

Why You Need a Strong Data Retention Program

Data retention is a cornerstone of any data management effort. Both internal and external policies dictate data retention rules and regulations, and it's critical for organizations to be able to manage a comprehensive data retention program that caters to both. Data privacy and protection regulations like the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), for example, establish specific requirements for the information organizations can retain — and what they need to delete — to protect sensitive consumer information, minimize individual privacy risk, fulfill data subject access requests, and more.

Companies aiming to avoid violations and strengthen customer trust need to define, manage, and remediate data retention policies across the business.

Solid Data Retention Programs Must:

- define data according to how long an organization should hold onto it
- distinguish critical information from redundant, obsolete, and trivial (ROT) data
- account for legally allowable exceptions to data retention requirements (such as pending lawsuits or audits)
- determine whether records should be archived or deleted
- maintain legal and IT teams to create and operationalize data retention policies
- provide a bridge between legal and IT teams so they can maintain constant communication, achieve compliance, and stay up to date with all regulations

> Companies aiming to avoid violations and strengthen customer trust need to define, manage, and remediate data retention policies across the business.

Data Retention Across the Organization

To adhere to — and prepare for — increasingly complex data retention policies, cross-functional teams from privacy, security, and governance offices must come together to design, enforce, and align data retention practices across the business.

Key Members for Your Data Retention Program Include:

- Policy creators: Usually on privacy, legal, records management, or compliance teams, policy creators design and manage policies according to privacy and protection regulations.
- Data owners: IT or business data owners review retained files in violation, determine and manage exceptions, validate DSAR fulfillment, or send data through remediation processes.
- Auditors: Internal or third-party auditors validate policies and violations and confirm remediation actions.

Define Your Data Retention Policies

Depending on your industry and business, multiple laws and regulations might affect your data retention policy — and they might call for overlapping, or even conflicting, requirements about how long you can maintain certain types of data, or what you must do with it when it's time to discard it.

In addition, different types of records may have different retention periods, adding another layer of complication to your data management efforts. A solid data retention policy should cover obligations under all applicable regulations — which can vary dramatically depending on the regulation, type of data, and more. For example:

Health Insurance Portability and Accountability Act (HIPAA)	HIPAA rules that organizations need to keep certain records for a minimum of six years. Additionally, there are state-specific laws that govern the retention of medical documents, and those requirements vary.
The Gramm-Leach Bliley Act (GBLA)	GLBA states that financial institutions must hold onto privacy notices forever, giving consumers the option of prohibiting third-party sharing of certain information.
Sarbanes-Oxley Act (SOX)	SOX stipulates that all business records be retained for no less than five years. This includes electronic records and messages.
Occupational Safety and Health Administration (OSHA)	OSHA includes a strict set of rules for data retention that include keeping personnel records for seven years after termination, medical exposure records for 30 years, and drug test records for one year. Organizations need to work closely and carefully with their privacy teams to ensure compliance with all regulations that apply to them — along with internal business policies for data retention.

How BigID Helps with Data Retention Challenges

For companies standing up a smart data retention strategy, a “keep it all” approach no longer works. Instead, organizations must selectively retain or delete data according to the regulations that apply to them based on industry, location, and other variables.

Knowing the data you have — and the risks associated with it — is the foundation of any data retention program. BigID catalogs, classifies, and correlates identity and entity data into profiles that you can access through a centralized and easy-to-use interface. BigID’s data retention app enables organizations to manage data retention across all of their data.

> **Knowing the data you have — and the risks associated with it — is the foundation of any data retention program.**

Discover and Inventory All Your Data

To determine which data to maintain or discard, you have to see all of it — the data you know about and the data you don’t, structured and unstructured, on-prem and in the cloud, across all data types, stores, and sources — all in one place.

Leverage ML-based discovery-in-depth to find and inventory all of your data by identity, content, type, and sensitivity — without copying or duplicating data. Map petabytes of data, everywhere, to decide what to delete and what to keep — and for how long.

Define and Apply Custom Policies to Retain or Discard Data

Discovering all your structured and unstructured data is just the beginning.

By applying in-depth classification to that data, you can build a catalog view of it all in one place. A robust data catalog enables you to create custom retention policies to act on aging data, including:

- tagging what information to keep
- setting up workflows to manage how long you can keep it, and
- marking over-retained data for deletion

This transparency facilitates operationalization efforts across the organization and empowers teams to create and define policies and business rules once — and then apply them consistently across all structured and unstructured data.

BigID supports policy types based on:

- time
- date created
- date modified
- content
- data type (e.g., email, documents, shared drives, etc.)
- organization
- geography
- sensitivity: PI, PII, content-based
- domain: entity-based
- environment
- precedence rules and management

and more.

BigID empowers your organization to create personalized workflows tailored to the needs of policy creators, data owners, and auditors.

Automate Workflows and Take Action on Your Data

Companies need to be able to report, review, and remediate data in violation.

To operationalize data retention workflows, organizations must apply the same policies and identify violations across different types of data — and leverage multiple ways to identify the same data across different data sources.

BigID empowers your organization to create personalized workflows tailored to the needs of policy creators, data owners, and auditors.

Leveraging BigID's deep discovery foundation, you can automatically translate legal and business requirements into policy definitions to be executed at the data source level. IT teams can then identify, track, prioritize, delegate, and take specific actions on policy violations — across different data sources.

Comply with Regulations that Apply to Your Organization

From the GDPR and CCPA to SOX for finance, HIPAA for health care, and multiple others, regulations that determine data retention are complex.

Customer records, contracts, financial information, healthcare data, third-party data, employee records, spreadsheets, emails, and more are all commonly regulated by data retention policies — regardless of industry.

With BigID, customers can easily identify and inventory all personal, critical, and regulated data to manage retention policies, findings, and violations. Incorporate individual DSAR retention periods, integrate with data remediation functionality to stay ahead of regulatory developments; and notify users of changes — all in one interface.

Start Building Your Data Retention Program

Organizations can leverage BigID's unmatched, ML-based approach to inventory their data by identity, content, type, and sensitivity so they can know the data they have and the risks associated with it.

By leveraging BigID's data retention app, they can create data retention policies for data aging, access report findings by data sources, send high-risk data to remediation workflows, manage policy violations, and operationalize policies across the organization.

Schedule a demo to learn more about how BigID can help with every aspect of your organization's data retention program across all of your data, everywhere.

> **By leveraging BigID's data retention app, they can create data retention policies for data aging, access report findings by data sources, send high-risk data to remediation workflows, manage policy violations, and operationalize policies across the organization.**