A BUYER’S GUIDE TO PRIVACY-AWARE DATA GOVERNANCE

Best practices for how data privacy and governance can work together to help you achieve full compliance and create real insights from data
## TABLE OF CONTENTS

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Power of Data</td>
</tr>
<tr>
<td>2</td>
<td>Privacy, Meet Data</td>
</tr>
<tr>
<td>3</td>
<td>Best Practices for Bringing Privacy and Governance Together</td>
</tr>
<tr>
<td></td>
<td><strong>a.</strong> Discover what data you have</td>
</tr>
<tr>
<td></td>
<td><strong>b.</strong> Define what the data is</td>
</tr>
<tr>
<td></td>
<td><strong>c.</strong> Classify what your data means</td>
</tr>
<tr>
<td></td>
<td><strong>d.</strong> Catalog data for context</td>
</tr>
<tr>
<td></td>
<td><strong>e.</strong> Tag data for maximum value</td>
</tr>
<tr>
<td></td>
<td><strong>f.</strong> Identify data provenance for risk management</td>
</tr>
<tr>
<td>4</td>
<td>Full Compliance, Real Insights</td>
</tr>
</tbody>
</table>
THE POWER OF DATA

Data is powerful. It’s used by organizations to make better business decisions, streamline operations, and reduce operating costs. Many of today’s Fortune 1000 companies transformed their business by recognizing and leveraging data as their most valuable asset.

Data has value that can drive business insights with the proper use and management, but that data — like all valuable things — also needs to be organized, protected, validated, and audited. It often contains sensitive information that could revolve around an individual, an organization, or even the value of a business.

Many of today’s Fortune 1000 companies transformed their business by recognizing and leveraging data as their most valuable asset.

In the age of the General Data Protection Act (GDPR) and the California Consumer Privacy Act (CCPA), organizations face new regulatory requirements for protecting and reporting on sensitive data. This, in turn, creates an urgent need for companies to better manage their data assets in the first place.

Organizations are enhancing their data governance programs to address this need. As part of that effort, it’s necessary for the privacy group and data office to collaborate more efficiently to manage, protect, and report on their organizations’ data.
For any organization that collects and processes customer, employee, or business-sensitive data — and wants to ensure that data remains as accurate, complete, and “true” as possible — the CDO can be the CPO’s best friend.

As it stands, companies may have gaps in their existing data management programs that present business challenges. To address these challenges, organizations need to:

- Know their data: identify what data they have — and where and whose it is
- Build a framework to identify and define what data is sensitive, personal, or regulated — and may be subject to privacy or protection regulations
- Discover and apply meaning and context around their data — for proper use and management
- Understand where their data comes from — and what it contains
- Bring their data together under one pane of glass to create insights and drive business value

The sheer amount of data generated on a daily basis can also create issues in efficiently fulfilling data subject access requests (DSARs), and that can only be fixed by addressing data governance.

Properly managed and governed data needs to not merely support — but improve — all of the organization’s business functions, including data privacy management. This translates into building a mature framework with repeatable and efficient processes that quickly respond to new — and sometimes conflicting — regulatory requirements.
There are several methods that privacy and data offices can use to create defensible programs for responding to regulatory and privacy threats.

**DISCOVER WHAT DATA YOU HAVE**

You can’t manage what you don’t know you have. The first step to privacy-aware data governance is discovering the data you have in the first place so you can take the proper steps to manage it.

**HOW TO DO IT**

Organizations need to be able to automatically discover data at petabyte scale, across all of their data sources. Deep data discovery builds the foundation for insights you can gain from it down the road.

**WHERE TO START**

To build up to the right data insights, you need the right infrastructure, and that means a deeply intelligent discovery foundation. Get unparalleled discovery-in-depth that combines multiple modes of discovery to uncover actionable context around all types of personal, sensitive, and dark data.
DEFINE WHAT THE DATA IS

Know what data you have and what it contains. Identify the discrete building blocks of all your data elements to find: definitions, purpose of use, business rules, business and data controls, business processes, data quality rules and scores, risk impacts, an ownership matrix, and more.

HOW TO DO IT

Define your data to help identify its value and use it for privacy requirements and various other uses. Integrate business, operational, and technical metadata - and link related and inferred data points for the big picture. You can’t report on data — or otherwise use it effectively — if you don’t know what information it contains.

WHERE TO START

Data elements can’t do much for you if you don’t know what they are. Use advanced machine learning to find and identify all sensitive and personal data, integrate metadata, and establish a single source of truth across your data landscape.
CLASSIFY

CLASSIFY YOUR DATA

Insights derived from your data are only as good as your understanding of that data. Classify your discovered and defined data to inventory it according to various attributes and settings, such as confidential, sensitive, internal — or by policy, custom tags, and more.

HOW TO DO IT

Identify and classify confidential, regulated, and sensitive data so you can treat it accordingly, better handle the risk associated with it, and ensure its compliance with privacy regulations. For example, you may want to assign different access levels or priorities around processing certain types of sensitive data — or classify by policy or information type.

WHERE TO START

Automatically apply multiple techniques to classify enterprise data, leveraging machine learning to understand relationships between data values — beyond just metadata.

Classify by person, identity, sensitivity, policy, regulation, and more: go beyond traditional pattern-based classification to capture and identify all types of sensitive and personal data.
Building context around your data is a critical part of determining how to manage it. A data catalog gives you a view of your discovered, defined, and classified data and its associated features.

**HOW TO DO IT**

A catalog view gives you insight into your data across your entire data ecosystem - and should integrate business context, data inventory, and technical insights for data governance initiatives. This facilitates greater accuracy, comprehensive insights, and shorter time to value.

**WHERE TO START**

*Catalog and map sensitive and personal data* in context with business, operational, and technical metadata.

From there, you’ll be able to get deep data insight, incorporating active metadata, data profiling and statistics, and classification — all within a single pane of glass for all types of data, both on-prem and in the cloud.
TAG DATA FOR MAXIMUM VALUE

Create categories in the data catalog that describe the purpose of usage for the data. Enable smarter, more accurate and automated policy enforcement decisions — helping optimize your investments and address new privacy requirements.

HOW TO DO IT

Effective tagging, or data labeling, enables smarter, more accurate policy enforcement decisions to help you address new privacy requirements. For example, both GDPR and CCPA mandate that a business must be able to describe its data’s purpose of use, and labeling allows you to do that.

WHERE TO START

Identify composite identity information with simple logical commands and tag in catalog for inventorying, analysis, and data monitoring.
IDENTIFY DATA PROVENANCE FOR RISK MANAGEMENT

Document the full journey of a data element, starting from the “authoritative” source to downstream sources and applications that store it, display it, or both.

**HOW TO DO IT**

Know a data element’s entire lifecycle, from where, when, why, and how it was collected, to every step it’s taken along its journey in your business.

**WHERE TO START**

Track and report on your data history and touchpoints throughout your company.

Understand the map and flow of how sensitive data moves around in your organization so that you can ensure early detection of breach vulnerabilities or privacy regulation violations.
FULL COMPLIANCE, REAL INSIGHTS

Any organization that processes data must do so in a responsible manner — prioritizing proactive protection and management of all sensitive and personal data. Data privacy and governance form an important intersection where that can happen — and where countless opportunities live.

The CPO and CDO together can create a defensible privacy framework that not only puts its business into full compliance but also provides value by creating real insights derived from data.

Find out more about how BigID empowers organizations to implement privacy-aware data governance, and how to automatically discover, classify, and catalog all types of data across an organization’s data landscape in a single pane of glass.

See how data and privacy can work together to reduce data silos, automate discovery, eliminate duplication of data, manage breach investigations, and leverage advanced reporting and analysis for all sensitive and personal data.

Create a defensible privacy framework that not only puts its business into full compliance but also provides value by creating real insights derived from data.