PRIVACY-AWARE GOVERNANCE: EMPOWERING TRUST, TRANSPARENCY AND TRANSFORMATION

Introduction

Today's increasingly complex data privacy regulations create new challenges for organizations. They must not only understand where personal and sensitive data lives within the organization and whose data it is, but also take action to ensure its collection and use is compliant. This amplifies the need for organizations to better understand what data they have. It is no longer sufficient to manage information – organizations must act ensuring they collect and use information in an automated way in accordance with privacy requirements.

The influx of consumer privacy regulations and the explosive growth of records are challenging organizations to rethink how they find, classify and manage personal information – especially with customer information residing in unstructured format on network drives including Microsoft® SharePoint, Microsoft 365 and Microsoft Teams opening organizations up to significant risk.

TABLE OF CONTENTS

WHY PRIVACY-AWARE GOVERNANCE?

The pace of proposal for and adoption of modern privacy regulations accelerated through 2020, surpassing the record-breaking cadence in 2019. This has raised the stakes for organizations looking to standardize a global policy when handling personal data. Organizations face increased financial, brand and compliance risks without a proactive approach to governing information, including adhering to GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act) and CPRA (California's Consumer Privacy Rights Act) compliance.

Meanwhile, organizations' IT environments continue to change, adding complexity to governance. Companies accelerated moving their applications and workloads to the cloud, driven by the pandemic and economic fallout, either to reduce in-person work at data centers or because the cloud offers more flexibility as business demands fluctuated. Now that IT leaders need to manage on-premises systems, public cloud, and hybrid-cloud IT environments, they face several compliance and data governance challenges with their content:

- They don't know where privacy information resides within documents and records
- They are unable to associate privacy information within records to a specific customer
- They have no audit record of who has accessed or viewed the privacy information
- They are not currently able to redact privacy information
- They are maintaining customer information for longer than required by law

Privacy regulation and a declining public reputation have been important drivers of organizations' efforts to protect personal data and avoid costly fines and penalties. Highly publicized data breaches have also contributed to data security concerns among customers. A report by McKinsey and Company reports 71%[1] of consumers would stop doing business with an organization that gave away sensitive data and a staggering 87% said they would not do business with a company they suspected of inadequate security practices.

According to a 2020 AIIM study[2], the amount of information coming into organizations will increase up to 4.5 times in the next 18 to 24 months – and 60% of that data will be unstructured. Knowing that content will only continue to grow, and the remote workforce is not going away, it is no longer enough for organizations to simply manage information. They must prioritize privacy and regulatory compliance in their governance strategies.

[1] McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019
[2] The State of Information Management in 2020, AIIM

87% of customers would not do business with a company they suspected of inadequate security processes.

PRIORITIZE PRIVACY-AWARE GOVERNANCE

To start, organizations need to gain visibility and transparency into where sensitive and personal information resides within their content, documents and records. With the sudden and drastic increase of a remote workforce, workers use shared/network drives, SharePoint and Microsoft 365 more than ever.

A new report[3] from DLA Piper shows that GDPR fines are being handed out more frequently, with a jump of 39% in 2020 over the previous year-and-a-half since the law went into effect. The total fine count to date for the whole of the European Union member states is £245.3 million (about $332.4 million), but there remains a strong disparity in the willingness of individual national regulators to issue fines with two countries responsible for over 50% of that amount.

As a result, IT leaders need to be concerned that ungoverned, user-managed documents and content puts the organization at risk. IT leaders can help with a privacy-aware governance approach for unstructured and structured data focused on:

1. **Helping leaders make the case.** Scanning and discovering where sensitive information resides in file shares, network drives, SharePoint, Microsoft 365 email, and more helps leaders understand and size potential risks to the organization. Technology such as OCR and other scanning tools exist today to help discover information quickly and cost effectively.

2. **Demonstrating how you can manage and govern what puts your organization at risk.** Organizations can scale their usage of content management platforms to manage the lifecycle of this information, including its removal. Today, federation capabilities also enable organizations to apply governance policies to information across repositories and shared drives. These policies can include redacting sensitive information, on the fly, to ensure personal information is used correctly and consistently.

3. **Funding through rationalizing content sprawl.** Organizations can achieve immediate savings and value by rationalizing and consolidating content repositories and systems putting them at risk. This rationalization and consolidation can also take advantage of private-cloud, hybrid-cloud, and SaaS-ready options to further reduce infrastructure spend.

[3] DLA Piper GDPR fines and data breach survey January 2021
[4] From Privacy to Prot: Achieving Positive Returns on Privacy Investments Cisco Data Privacy Benchmark Study 2020

> For every $1 an organization invests in privacy spending, it receives an average $2.70 return on investment, according to a 2020 Cisco study[4] that asked privacy professionals across various industries in 13 countries to estimate their privacy investments' financial benefits.

EMPOWER INFORMATION DISCOVERY, CLASSIFICATION AND ACTIVITY

With the explosive growth of records and the advent of widespread remote work due to the pandemic, organizations need to rethink how they find, classify and manage personal information. For instance, as remote workers use shared/network drives, SharePoint and Microsoft 365, there are concerns with user-managed documents not being classified properly.

When it comes to content management, the top challenges organizations report facing relate to lacking the right data governance tools and processes. According to respondents in a recent survey[5], the top challenge is employees saving content on shared drives/personal drives (41%), which we know is happening at 58% of respondents' organizations.

But it is no longer enough for organizations to simply manage information. They must elevate their governance strategies – knowing what data they have and ensuring they collect and use that data in accordance with privacy regulations.
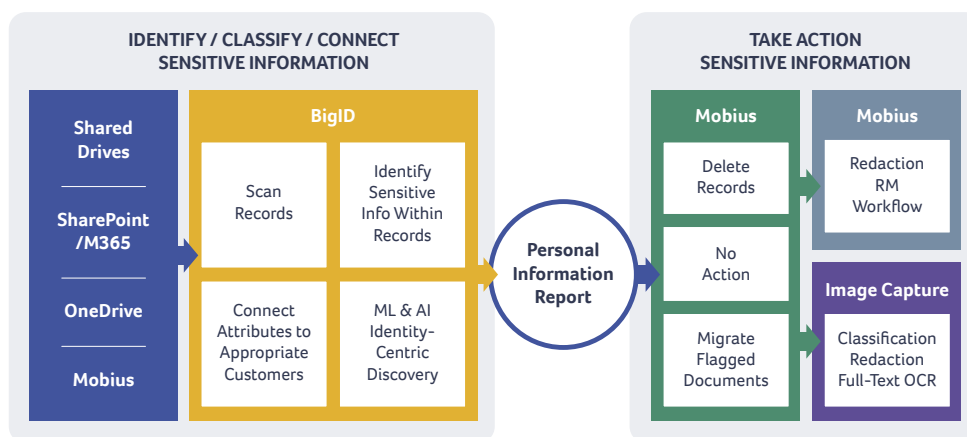
To start, organizations need to gain visibility and transparency into where sensitive and personal information resides within their documents, content and records. However, most currently lack the ability to identify where that information exists within content. Even if they could, most organizations are unable to associate personal information within records to a specific person – making it near impossible to adhere to consumer requests for deletion.

Organizations need an integrated solution that addresses both structured and unstructured content and can:

- Scan and discover where sensitive information resides
- Properly manage the access, storage and deletion of sensitive information
- Automate migration, legal holds, redaction and disposition policies based on classification insights
- Extend information governance and data privacy to shared drives, SharePoint and Microsoft 365

By transforming their governance strategy for content, organizations can operationalize compliance. Doing so not only helps contend with privacy regulations, but also supports digital transformation.

PRIVACY-AWARE PROCESS FLOW

IDENTIFY / CLASSIFY / CONNECT SENSITIVE INFORMATION			TAKE ACTION SENSITIVE INFORMATION		
Shared Drives / **SharePoint /M365** / **OneDrive** / **Mobius**	**BigID** Scan Records / Identify Sensitive Info Within Records / Connect Attributes to Appropriate Customers / ML & AI Identity-Centric Discovery	→ Personal Information Report →	**Mobius** Delete Records / No Action / Migrate Flagged Documents	**Mobius** Redaction RM Workflow / **Image Capture** Classification Redaction Full-Text OCR	

[5] ASG Technologies 2021 Survey Report: What's Slowing Modernization? *Barriers Hindering Enterprise IT Systems and Content Management*

LEVERAGE AUTOMATION IN DATA GOVERNANCE

Many large, highly regulated organizations are turning to automation to improve their content management and compliance efforts. Across industries, companies are increasing investments in machine learning (ML), robotic process automation (RPA) and artificial intelligence (AI) to make data governance more agile and automated. Automation empowers organizations to respond to the growing needs for security and compliance, as well as process improvements that can enhance company performance and efficiency. Leveraging automation for governance does not just support compliance efforts, it also translates directly to the bottom line.

There are three best practices to take advantage of automation and boost records management and compliance:

1. **Identify where automation can help.** AI and RPA can seem futuristic, but they are already applicable and available for today. Organizations must start by understanding the current processes in play and identifying which are good candidates for automation.

2. **Automate gaps where automation has not been applied.** Many organizations adopted process automation to support specific workflows or isolated departmental duties. However, at the same time, many key business activities still require manual data entry. Organizations can replicate the automation technologies from one area to these other applications.

3. **Adopt continuous auditing and analytics.** Information must be governed throughout its entire lifecycle. Organizations should avoid projects that are executed in siloes. Instead, they can use continuous auditing and analytics to monitor and improve compliance, enhance efficiency and reduce the need for one-off cleanup efforts.

Records management, process automation and compliance are all on the rise, and organizations must use a holistic approach to success. Looking for partners and providers with the right mix of expertise, capabilities and vision will allow organizations to maximize their efforts.

AUTOMATION BENEFITS

- Up to 95% classification accuracy with AI/ML

- 60% cost reduction in handling customer removal requests

- 30-50% reduction in operational costs/efforts

- 30% less overhead to scan unstructured/ structured at scale

CONCLUSION

As the GDPR, CCPA, CPRA have shown, data privacy regulations will only keep coming — and they will be increasingly targeted, have international implications and are perhaps even stricter. The latest batch of data privacy regulations points out companies' greatest IT and operations weaknesses, especially a lack of a unified view into business and how end users interact with documents and content. By implementing a privacy-aware information management strategy, for both structured and unstructured data, organizations can understand their entire ecosystem. It is increasingly important to proactively seek out dark data, tackle compliance and prepare for current and future data privacy regulations.

asg
technologies®

ASG_Privacy-AwareContentGovernance_20210225en