Published by COMPLIANCE WEEK

Tech's role in changing data privacy compliance landscape

An e-Book sponsored by exterro®

About Us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a quarterly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

exterro®

Exterro empowers legal teams to proactively and defensibly manage their Legal Governance, Risk and Compliance (Legal GRC) requirements. Our Legal GRC software is the only comprehensive platform that automates the complex interconnections of privacy, legal operations, digital investigations, cybersecurity response, compliance, and information governance. Thousands of legal teams around the world in corporations, law firms, managed services providers and government and law enforcement agencies trust our integrated Legal GRC platform to manage their risks and drive successful outcomes at a lower cost. For more information, visit www.exterro.com.

Survey: Tech key to compliance in changing data privacy landscape

Respondents to a survey from Compliance Week and Exterro largely said they were confident their organizations are meeting regulatory requirements regarding data privacy despite evidence their data retention policies and procedures are outdated.

BY ALY MCDEVITT, COMPLIANCE WEEK

When it comes to keeping up with data privacy regulation, organizations would be wise to adopt a more comprehensive technology solution to drive efficiency and minimize human error.

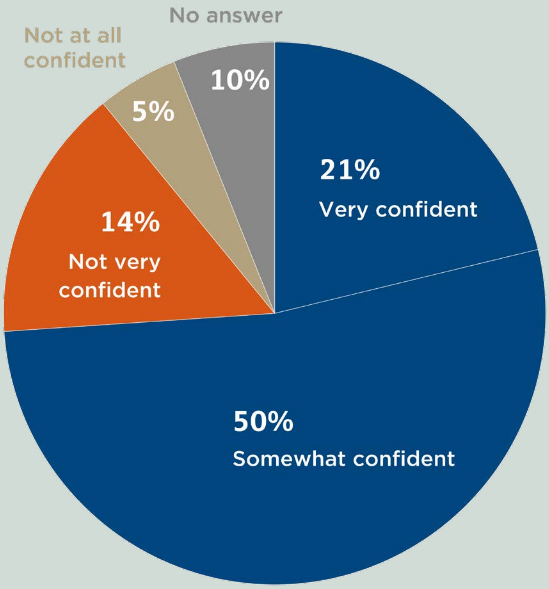
Companies farther along the data privacy maturity curve recognize this wisdom and are more proactive about embracing data management technology in-house.

This anecdotal observation notwithstanding, most companies still hold fast to data compliance policies and procedures that depend on personnel for manual implementation and upkeep, according to a new survey from Compliance Week and information governance software provider Exterro.

The "Data Retention in 2023" study, conducted online between January and February, surveyed 173 senior-level executives, directors, managers, and analysts in the compliance, audit, risk, and information security professions. More than 30 industries were represented in the sample, with the largest constituent of respondents working in financial services (31 percent). Company sizes ranged from small, with fewer than 1,000 employees (43 percent); to midsize (31 percent); to large, with 10,000-plus employees (25 percent).

Among the key findings was evidence of false confidence in how well organizations are staying abreast of the dynamic data privacy regulatory landscape. Nearly three-quarters (71 percent) of respondents indicated they are "somewhat" to "very" confident their company is meeting all applicable

How confident are you that your data retention processes or solution are meeting all applicable state and international regulatory requirements?



> "Records retention is no longer a puzzle a human can solve. It leads to a false sense of compliance and, potentially, delays in cleaning ROT (redundant, obsolete, and trivial) data, which can adversely impact any business—for example, in the case of a breach."
>
> Amalia Barthel, Partner & VP Compliance, Wareness Canada

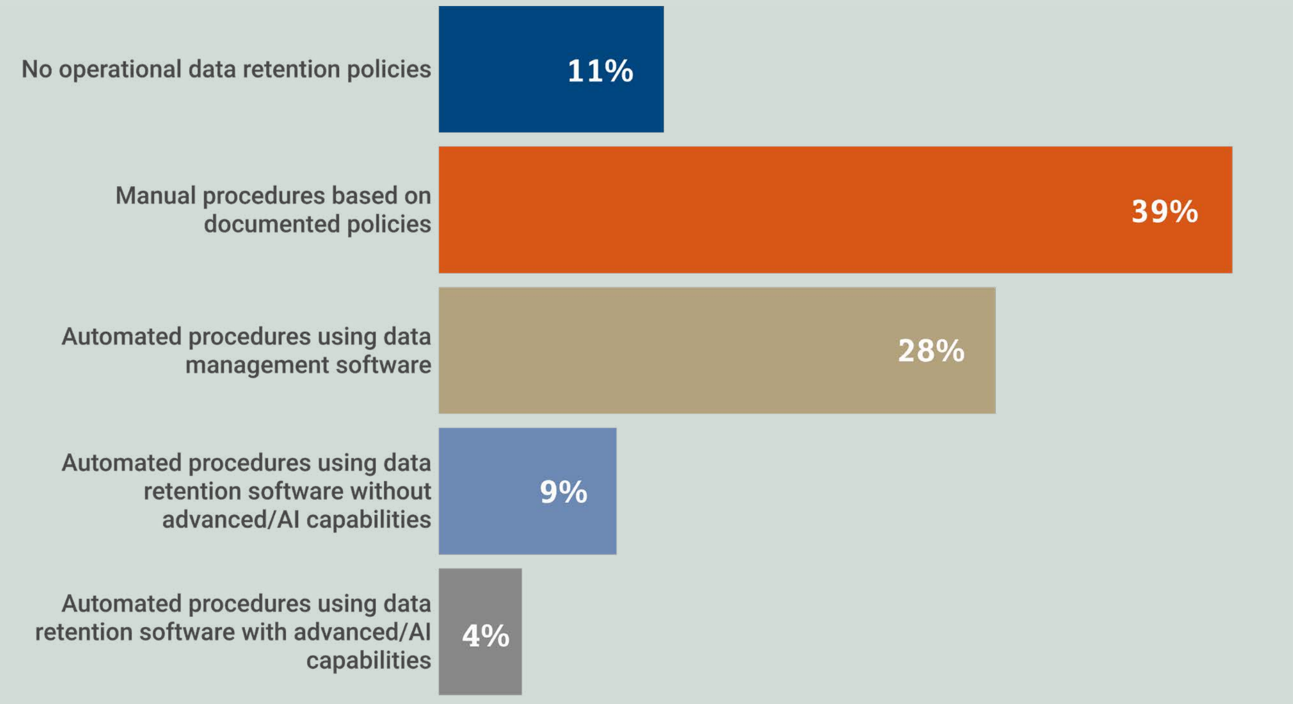
state and international regulatory requirements regarding data privacy.

Yet, on the whole, respondents' data retention policies and procedures are decidedly outdated, falling behind the times with an overreliance on human resources. Half (50 percent) of all respondents described their data retention policies and procedures as fully manual (39 percent) or nonexistent (11 percent).

Further, the majority of companies rely on human resources to put their data retention policies into action, as 63 percent of respondents indicated their company relies on line of business data holders or centralized IT workers to implement policies across the enterprise—as opposed to using technology to automate the scanning, classification, and deletion of data according to appropriate retention schedules.

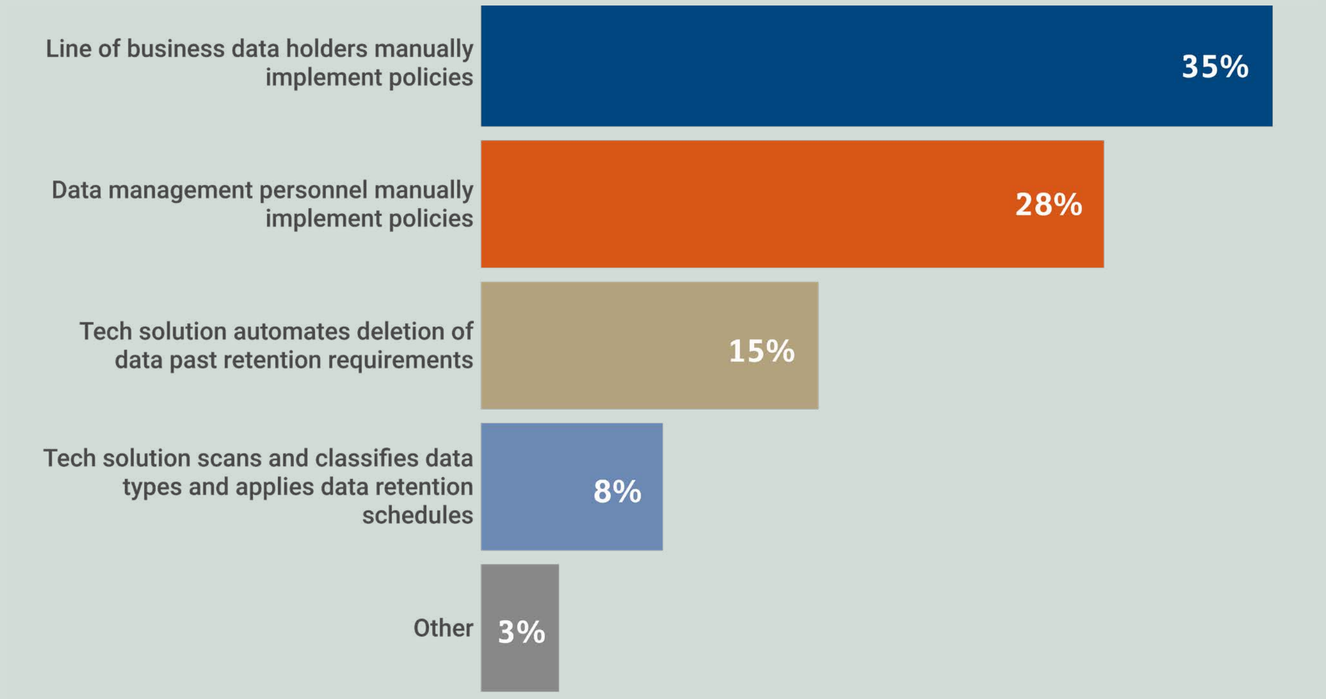
When asked how their company ensures its data retention policies and procedures reflect the most recent applicable state and international requirements, 78 percent of respondents said their organization relies fully on legal, privacy, or IT personnel to make the necessary updates. Just 8 percent of respondents indicated their company leverages technology to automatically apply new regulatory requirements to appropriate data types.

Describe your data retention policies and procedures.



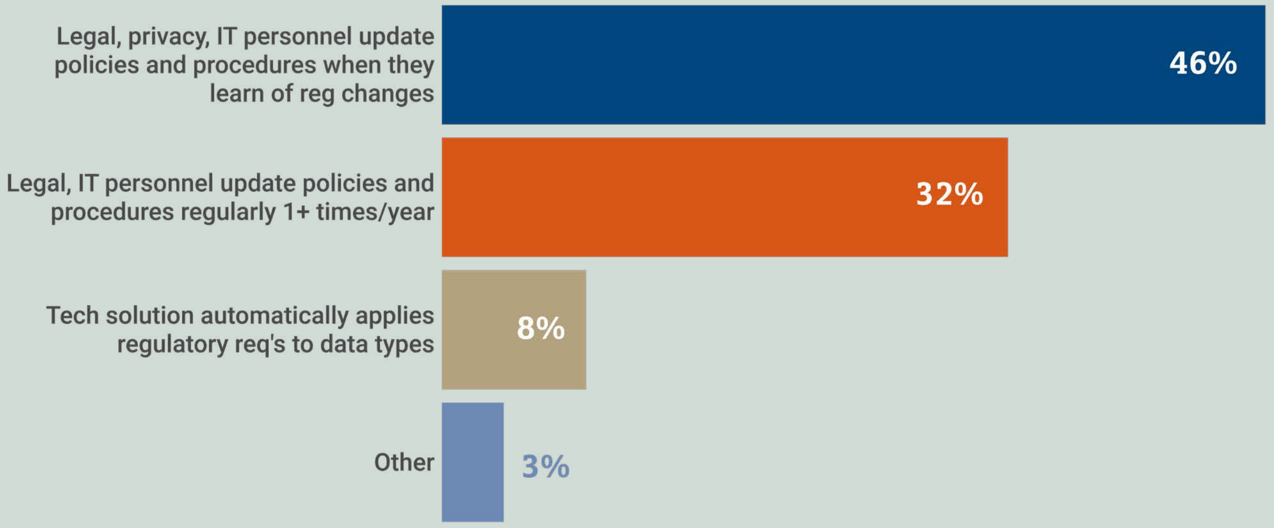
Note: 9% did not answer

How do you put your data retention policies into action?

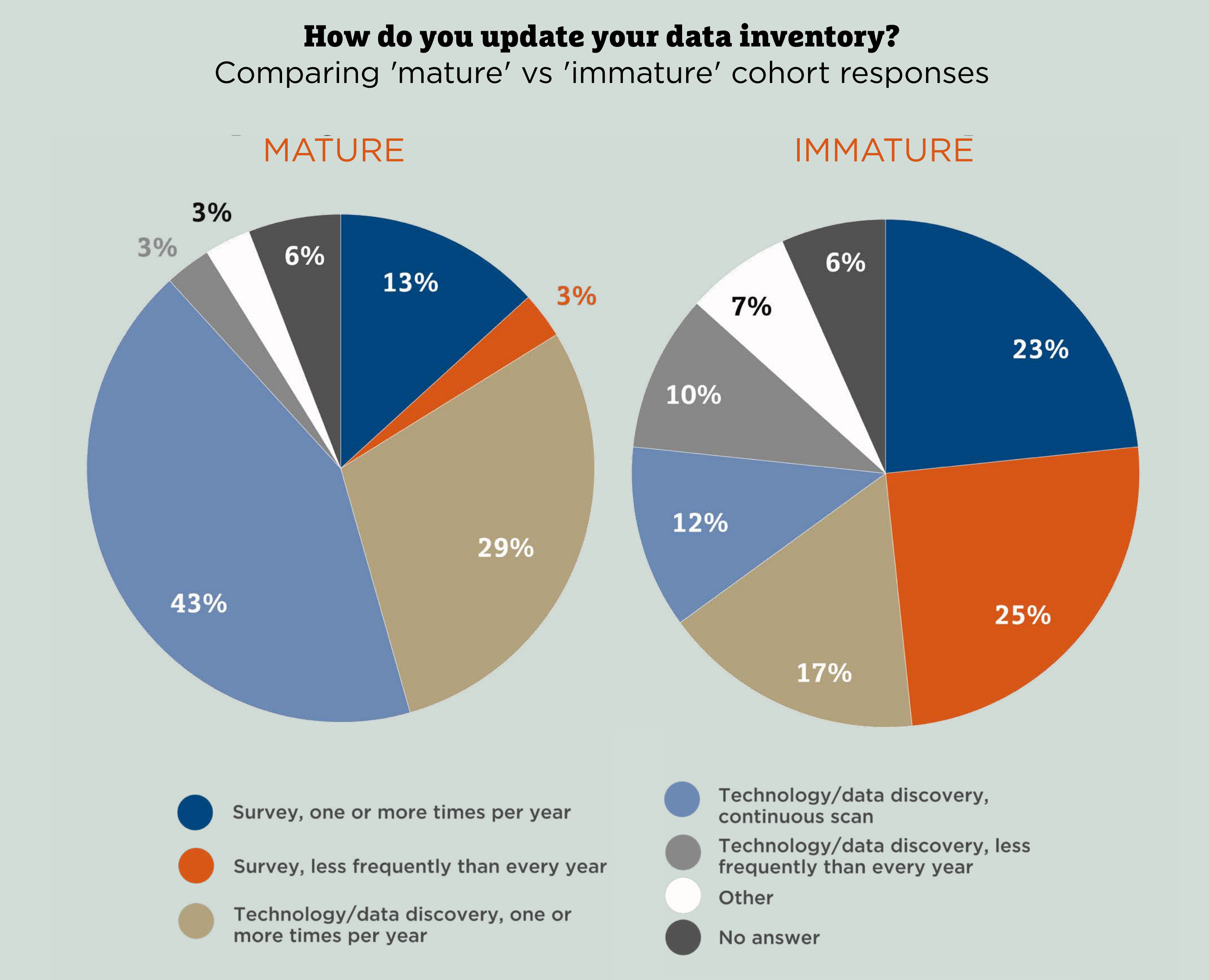


Note: 11% did not answer

How do you ensure your data retention policies and procedures reflect the most recent applicable state and international requirements?



Note: 11% did not answer



How do you update your data inventory?
Comparing 'mature' vs 'immature' cohort responses

"Records retention is no longer a puzzle a human can solve," warned Amalia Barthel, lecturer at University of Toronto and Partner & VP compliance at Wareness Canada. "It leads to a false sense of compliance and, potentially, delays in cleaning ROT (redundant, obsolete, and trivial) data, which can adversely impact any business—for example, in the case of a breach."

Relying on manual processes also means the company's institutional knowledge resides with personnel, not the organization.

"People move around, and when they leave, that knowledge walks out the door if you don't have systems in place. Technology helps retain that institutional knowledge," said Alan Friel, global data practice chair at law firm Squire Patton Boggs.

Few organizations are leveraging artificial intelligence (AI) to implement data retention policies and procedures, according to the survey data. Just 4 percent of respondents indicated their companies as leveraging automated procedures using dedicated data management software that includes capabilities to intelligently implement policies based on data types, business record types, and updated regulations.

"AI is very useful when good data and good AI governance is taking place," said Barthel. "Organizations are reluctant to use AI because of the uncertainty of the results. But there are tools that have invested in training and constantly checking the knowledge in their AI platforms, and the results provide incredible return on investment."

Just as heavy dependence on human knowledge is a risk

> “People move around, and when they leave, that knowledge walks out the door if you don’t have systems in place. Technology helps retain that institutional knowledge.”
>
> Alan Friel, Global Data Practice Chair, Squire Patton Boggs

to organizations, ungoverned reliance on technology is a hazard, too.

“The use of technology tools to find and manage data fills the gaps that will be inherent in relying on human knowledge,” said Friel. Nevertheless, “Reliance on technology cannot be a substitute for good due diligence with the stakeholders. Companies need to do both.”

Friel said the use of technology for information governance is a sign of a mature program, but, “We’re at a point where most companies have not reached a state of meaningful maturity.”

The data bears out the consensus technology drives efficiency. Respondents who ranked their company’s data compliance processes as more mature were about twice as likely to say their company uses technology to manage data. Of the 68 respondents who ranked their company’s data compliance processes as “managed” or “optimized,” 75 percent indicated their company uses technology to update data inventories—compared to just 39 percent of the 60 respondents who ranked their company’s data compliance processes as “ad hoc” or “repeatable.”

In-house technologies

According to the survey results, the most common privacy functions managed by companies’ in-house technologies are data retention and deletion (64 percent), third-party risk management (55 percent), and data breach response (52 percent).

Your technology solution should be able to answer 3 questions:

1. What data do I have?

2. What are the rules on retention?

3. How do I make sure I don’t over-retain?

For companies looking to move on from spreadsheets and calendar notifications and upgrade to a technology tool to facilitate data privacy compliance, they will want to ask themselves and be able to answer the following questions, according to Friel:

1. “‘What data do I have?’”
2. “‘What are the rules on retention?’”
3. “‘How do I make sure I don’t over-retain?’”

The ability to inventory and manage data and apply retention rules to identified data sets is the most important capability a tool can provide, added Friel, which corresponds with the survey findings. Respondents, where applicable, identified the top capabilities of their company’s data retention solution as: 1) applying regulatory requirements to relevant data types (35 percent) and 2) scanning and identifying data types across the enterprise infrastructure (31 percent).

More than a quarter of all respondents (28 percent) said their company does not have data retention software.

For companies shopping for such tools, Barthel offered a warning: Be on the lookout for data retention tools that overpromise and underdeliver.

“I reviewed many tools which claim they ‘do data retention.’ Regulations require that retention be examined by a data set, and I have not seen many tools capable of doing just that. In addition, I would not want an empty shell with just ‘guidance’ because organizations need to accelerate their data retention capabilities,” said Barthel.

The bottom line is companies need a system that triggers the deletion or destruction of data consistent with the retention periods to avoid the risks associated with holding onto data too long, whether that be a data leakage, data breach, or regulatory violation.

“You can have a retention schedule, but if you don’t have a system for applying it, then you don’t have a retention program. You have to have a way to apply the rules to the data set so that you don’t retain longer than the applicable periods. Otherwise, it’s just a policy on paper sitting in a drawer and not being implemented,” said Friel. ■

exterro®

FILLING IN YOUR BLIND SPOTS:

IMPLEMENTING A SUCCESSFUL DATA RETENTION PROGRAM

AN EXTERRO PRIVACY WHITEPAPER

CONTRIBUTORS

SHERYL FALK,
Partner, Winston & Strawn

CHRIS COSTELLO,
Senior E-Discovery Attorney, Winston & Strawn

AMY OLIVARES,
Manager, Corporate Governance & Compliance, Blount International

MORE DATA, MORE RESPONSIBILITIES

Modern organizations have embraced the notion that data has value. Business leaders focus organizational time and attention on capturing this value. In addition, technological change enables the IT community to radically reduce the costs of keeping and processing information. This creates new opportunities to collect more detailed data and to predict the behavior of systems, machines, and people. But along with value and costs come risks.

Data risk was once thought of as a technical challenge. However, the onslaught of data breach and data privacy legislation, and subsequent litigation, have changed this outlook. While the technological challenges remain and have even increased, managing the compliance and legal risks associated with data has become paramount. These activities are driving new strategies and new operating practices within legal and compliance organizations, and the businesses that serve them.

Advice about managing these risks is abundant. Interestingly, the legal, privacy, regulatory, and technical risks tend to be addressed separately. This is understandable, as different teams often look after these responsibilities. However, there is one activity that everyone is aware of which, if well-executed, can lower technical, legal, and privacy risks and increase compliance: a data retention/deletion program. Most organizations have defined a reasonable complement of data retention policies. But frequently these policies are not put into effect. There are many reasons for this, and overcoming these behaviors is a significant part of implementing a data retention program.

Data protection laws mandate that organizations remove data they no longer need, and this is a well-established best practice for security. Privacy laws also insist that personal information not be kept beyond its legitimate use or legal requirement, and newer ones are insisting that these retention periods be disclosed at collection time. Clearly, operational data retention is a necessary part of compliance with these regulations. It also helps reduce legal risk, as data that is defensibly deleted does not need to be produced by the organization in any subsequent discovery. And it helps with technological risk, because it is impossible to lose what isn't there.

WHERE WE ARE TODAY

Most organizations have a portfolio of data retention policies, and many have retention schedules. But in practice, the policies and schedules are not always used effectively and do not focus on data minimization. This results in a lax or haphazard approach toward data retention. Four challenges contribute to this dilemma.

1. ***Outdated ideas and approaches:*** **The traditional static approach to the retention schedules and processes fails to keep pace with the changing nature of data risks and data minimization best practices.**

2. ***Incomplete understanding of requirements:*** **organizations have only a fragmentary or siloed understanding of their data sources and retention obligations, resulting in incomplete inventories and operational inefficiencies.**

3. ***Complex regulatory landscape:*** **the passage of both the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) are painting a clearer picture of data retention obligations. Similar laws in Colorado and Virginia increase this pressure.**

4. ***Increasing variety of cyberthreats:*** **The increase in successful and attempted ransomware and data breaches compels organizations to implement data loss prevention measures that protect existing data from both internal and external security risks. Reducing the volume of redundant data held by the organization is one of the simplest means of reducing risk exposure.**

WHILE OPERATIONAL DATA RETENTION MITIGATES RISK

The legal risks associated with personal information are significant. Nearly all privacy and breach lawsuits, whether individual or collective, are based on the over-retention of data. The reasons for this are simple: Explaining to a jury why a data security or privacy scheme is inadequate is a complex and technical task, and unlikely to succeed. But explaining that data was kept longer than it should have been is straightforward. Privacy and data protection laws require disposing of data when it is no longer needed, so this is a valid complaint in every jurisdiction. An effective means of mitigating legal risk is implementing a defensible data retention program.

A defensible data retention program that is fully operational also mitigates another data privacy risk. Fulfilling "right to be forgotten" requests continues to be a struggle for many organizations. A major stumbling block is how to avoid deleting data that must be retained for other reasons.
A legal hold is often cited, but there are countless other global regulations that demand specific retention periods for certain types of information. Having a comprehensive data retention program will not only remove data that is not needed, but also preserve data that must be kept.

To implement an operational data retention program, organizations can follow these four steps:

1. Create an accurate data inventory
2. Develop an actionable retention schedule
3. Invest in the operational capabilities
4. Implement and enforce the program

STEP 1 CREATE AN ACCURATE DATA INVENTORY

Identifying and describing organizational assets in a data inventory is the critical first step in creating a data retention program. Without a solid data inventory, it is impossible to understand the scope of the data retention program and to build a path to implementation.

Three basic categories of information should be included in any data inventory:

- **An asset inventory, which most people think of as a data inventory, consists of a list of databases, tables, columns, file shares, and other technical artifacts that make up an organization's data.**
- **A process inventory identifies the processes that use data in the organization and the relationships among those processes, for example, the processes relating to the collection, use, and destruction of personal data.**
- **A record type inventory identifies the data types present in an organization, such as personnel records or financial records, rather than specific data fields in those records.**

STEP 2 DEVELOP AN ACTIONABLE RETENTION SCHEDULE

Your data retention schedule should reflect business priorities first, while also ensuring regulatory compliance. Industry best practices are a good guideline. In most areas there are established practices for common record types, which can be used as a starting place for schedule development.

To understand the business imperatives driving your data retention process, you must answer three main questions.

- **Why do we collect this data and what is its business purpose?**
- **Does the data fulfill that original business purpose?**
- **What business processes would be negatively impacted if we no longer retained the data in question?**

Recent regulations require organizations must have a clear-cut purpose for retaining data; data held onto for its own sake is a liability, not an asset.

STEP 3 INVEST IN THE OPERATIONAL CAPABILITIES

The organization must have in its arsenal a complete portfolio of operational capabilities including:

- **Data discovery**
- **Deletion validation**
- **User notifications and attestations**
- **Communications with document storage vendors**

Retention teams must ensure that these capabilities exist and can be used effectively to support the data retention schedule. If these capabilities are distributed throughout the organization, then processes and handoffs must be defined to ensure their correct execution, and roundtrip status must be available.

STEP 4 IMPLEMENT AND ENFORCE THE PROGRAM

The final step is to implement the program. To succeed, it must have clear responsibilities, defined performance metrics, and executive accountability.

Retention schedules must be revisited at least yearly and always in response to significant changes in data and business processes. Data retention management is an ongoing responsibility.

Each iteration of the program is the same as described here: update the data inventory, the schedule, the operational procedures, and the program itself. In addition to keeping your data retention program current, this cycle also enables continuous improvement.

The initial pass through these steps may be a substantial project; it isn't complete after one iteration. Organizations must repeat the process often to keep up with changes in data types, applications, regulations, and business processes.

The rate of change within your organization will determine the amount of effort required on an ongoing basis, future iterations of developing and implementing rules will be faster, as they build upon the foundation set by a data retention program.

Talk to an Exterro privacy expert today to jump start your data retention progam.

DATA RETENTION IS THE PRIVACY ‘ICEBERG’ THAT COULD SINK YOUR SHIP.

You need a programmatic, team-oriented approach, with a thorough understanding of your data and retention obligations at the center.

With this in place, you can:

- Fullfill data subject access requests
- Respond to breaches quickly
- Document compliance with regulations like CPRA and GDPR

Download Exterro’s Data Retention Handbook

exterro®

www.exterro.com