KPMG

Foundations of effective data retention and deletion

kpmg.com

Introduction

With the digitization of business operations, the emergence of new technologies for data storage and processing, generative artificial intelligence models and tools, and the growing importance of data in modern business decision-making, organizations are accumulating data at an exponential rate, creating an expanding data landscape. These data sets can be valuable for analysis and strategic decision-making, but their sheer volume can become unwieldy and expose a company to unnecessary risk without effective retention and deletion management. Ineffective retention and deletion leads to regulatory scrutiny, risk of data breach, inefficiencies, unnecessary storage costs, and reputational risks. Effective retention and deletion aims to organize and maintain data for as long as the data has business value and/or a regulatory requirement to retain. To enable effective data retention and deletion, businesses should consider adopting retention and deletion leading practices, allowing businesses to harness the most value from their data, meet regulatory expectations, and maintain consumer trust.

Balancing your data offense and data defense agendas

Effective data management is about balance—maintaining a stable equilibrium between your data offense and defense agendas. While a strong offense is advantageous in delivering valuable insights, defining new opportunities, and gaining or maintaining a competitive edge, a weak or discounted defense can expose your business to significant risks such as data breaches and legal or regulatory actions. On the other hand, prioritizing your defensive agenda at the expense of your offensive agenda may lead to impeded business operations, decreased productivity, missed opportunities, or unrealized profitability.

Therefore, it is vital for your organization to adopt a well-balanced data management strategy, allowing your business to leverage data offensively, proactively seeking insights, while simultaneously safeguarding your data against internal and external threats, and accounting for legal and regulatory obligations. By striking this balance, your business will be better positioned to spur innovation, excel in a competitive market, and drive profits while protecting your organization from potential threats posed by a complex, ever-evolving data landscape.

Striking a balance – Implementing leading practices across the data lifecycle

Effective retention and deletion starts at data creation. Businesses should consider adopting retention and deletion leading practices across the data lifecycle—creation, retention, and deletion. At KPMG LLP (KPMG), we understand your data is a valuable asset that should be managed in accordance with a balanced offense and defense. Our approach enables a balanced offense and defense through the below leading practices:

Retention schedule: Implementing policies which outline how long data should be kept, when it should be disposed of, considering legal, regulatory, and business requirements. Retention classes should be broadly defined and should include trigger events that are appropriate for the retention class.

Repository requirements: Detailing specifications for data storage locations, including archiving, making sure that data is secure and accessible, comports with legal and regulatory requirements, and adheres to retention and deletion schedules.

Data access management: Controlling, monitoring, and governing access to data and systems. This involves defined privileged access roles, monitoring user activities, authenticating identities, and enforcing authorization protocols.

Inventory of repositories requiring retention: Cataloging storage locations for data, enabling the demonstration of adherence to legal, regulatory, and company retention requirements. The inventory contains details on data types and retention protocols**.**

Legal holds management: Preserving data that may be relevant to legal investigations, cases and/or audits, suspending its disposal or deletion until the matter is resolved, and providing notice to safeguard data.

Collection and usage requirements: Aligning privacy requirements regarding collection and usage to data retention and deletion policies and procedures to enable your organization to uphold its privacy promise.

Performing and evidencing deletion: Deleting data securely and capturing evidence to support compliance with retention requirements, deletion safeguards, and governance processes. Evidence may include deletion logs, validating the deletion scope was fulfilled based on an established governance process.

Deletion framework: Defining a set of procedures and controls that guides the secure deletion of data in accordance with legal, regulatory, and business requirements.

Requirements to delete: Identifying and documenting the criteria for data deletion, such as data classifications and maximum retention periods. The criteria allows for the prioritization of deletion while supporting legal, regulatory, and business requirements.

Why act now?

Implementing effective retention and deletion practices reduces risks, improves regulatory compliance, eliminates unnecessary data, integrates business processes, and allows for cohesive retrieval, among other benefits. A detailed view into a range of the significant benefits that our clients have achieved, as a direct result of adopting the aforementioned leading practices and making significant investments in their retention and deletion programs, is captured in the visual below.

Reduction in risk and fines:

Reduces cost and risk in litigation discovery, reduces exposure to regulatory fines for lack of governance, and mitigates risk to actions based on failure to meet "privacy promise"

Improvement in regulatory compliance:

Helps with data retention in compliance with identified regulatory requirements

Thorough retrieval:

Allows data to be available and retrieved in an accurate, secure, and timely manner to satisfy business needs or for regulatory or legal review

Improvement in efficiency:

Reduces the time that employees spend copying, indexing, or retrieving data

Integration into business process:

Integrates the data lifecycle into corporate infrastructure and business processes, enabling compliance

Improvement in accurate identification:

Enables data across the organization to be accurately identified and assigned retention requirements

Reduction in storage costs:

Reduces storage cost over time, based on data minimization

Elimination of unnecessary data:

Eliminates redundant, obsolete, and trivial (ROT) data, mitigating the impact of future data security events and reducing cost

KPMG provides Retention and Deletion Enablement services, allowing clients to effectively manage data throughout its lifecycle

Reap the key benefits by working with KPMG. We offer a range of services, tailored to meet your organization's retention and deletion obligations and goals.

01 **Maturity assessment roadmap**

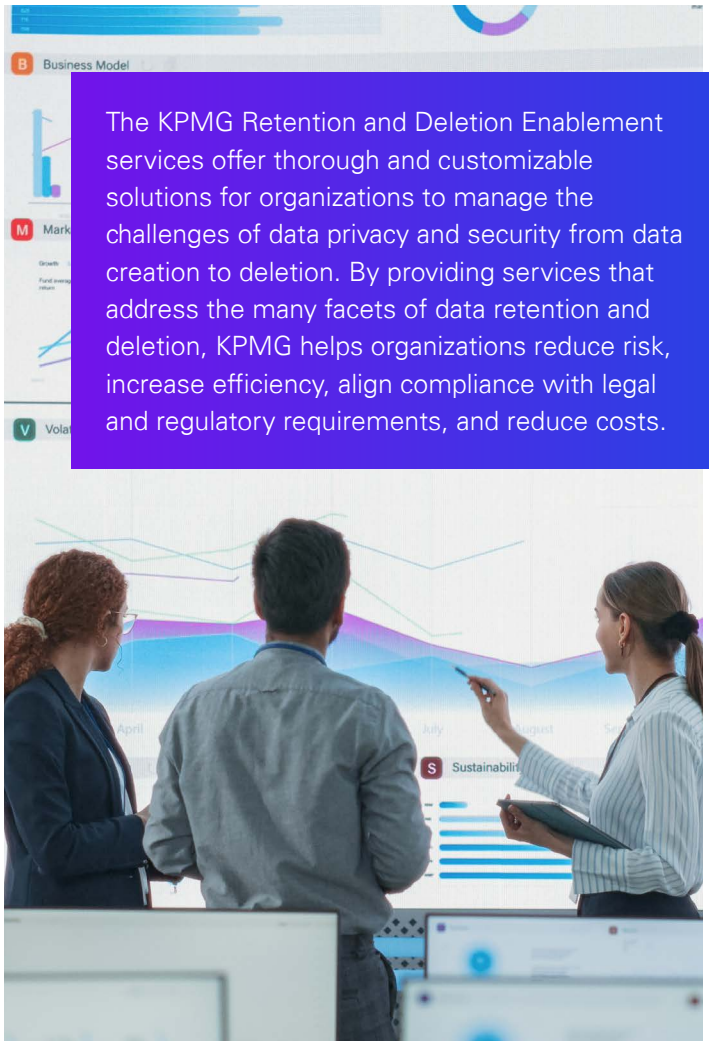
02 **Function implementation and transformation, including roles and responsibilities across the lines of defense**

03 **Use case development and requirements (including PI identification and remediation), tooling selection, and implementation**

04 **Regulatory response**

05 **Implementation of defensible disposition framework and associated process**

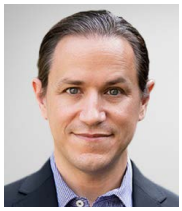
06 **Active support for legacy data disposition**



The KPMG Retention and Deletion Enablement services offer thorough and customizable solutions for organizations to manage the challenges of data privacy and security from data creation to deletion. By providing services that address the many facets of data retention and deletion, KPMG helps organizations reduce risk, increase efficiency, align compliance with legal and regulatory requirements, and reduce costs.

Contact us

Orson Lucas
Principal, Cybersecurity and Tech Risk
KPMG LLP
704-502-1067
olucas@kpmg.com



Rik Parker
Principal, Cybersecurity and Tech Risk
KPMG LLP
917-679-7103
rikparker@kpmg.com

Stephen Bartel
Director, Cybersecurity and Tech Risk
KPMG LLP
216-875-8038
sbartel@kpmg.com

Lee Merrill
Director, Cybersecurity and Tech Risk
KPMG LLP
904-354-5671
lmerrill@kpmg.com

Manoj Thareja
Director, Cybersecurity and Tech Risk
KPMG LLP
480-459-3682
mthareja@kpmg.com

Ben Bukai
Senior Associate,
Cybersecurity and Tech Risk
KPMG LLP
845-238-7692
bbukai@kpmg.com

Ashley Ryan
Senior Associate,
Cybersecurity and Tech Risk
KPMG LLP
470-514-6539
ashleyryan@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: **kpmg.com** **Subscribe**

DASD-2024-15772