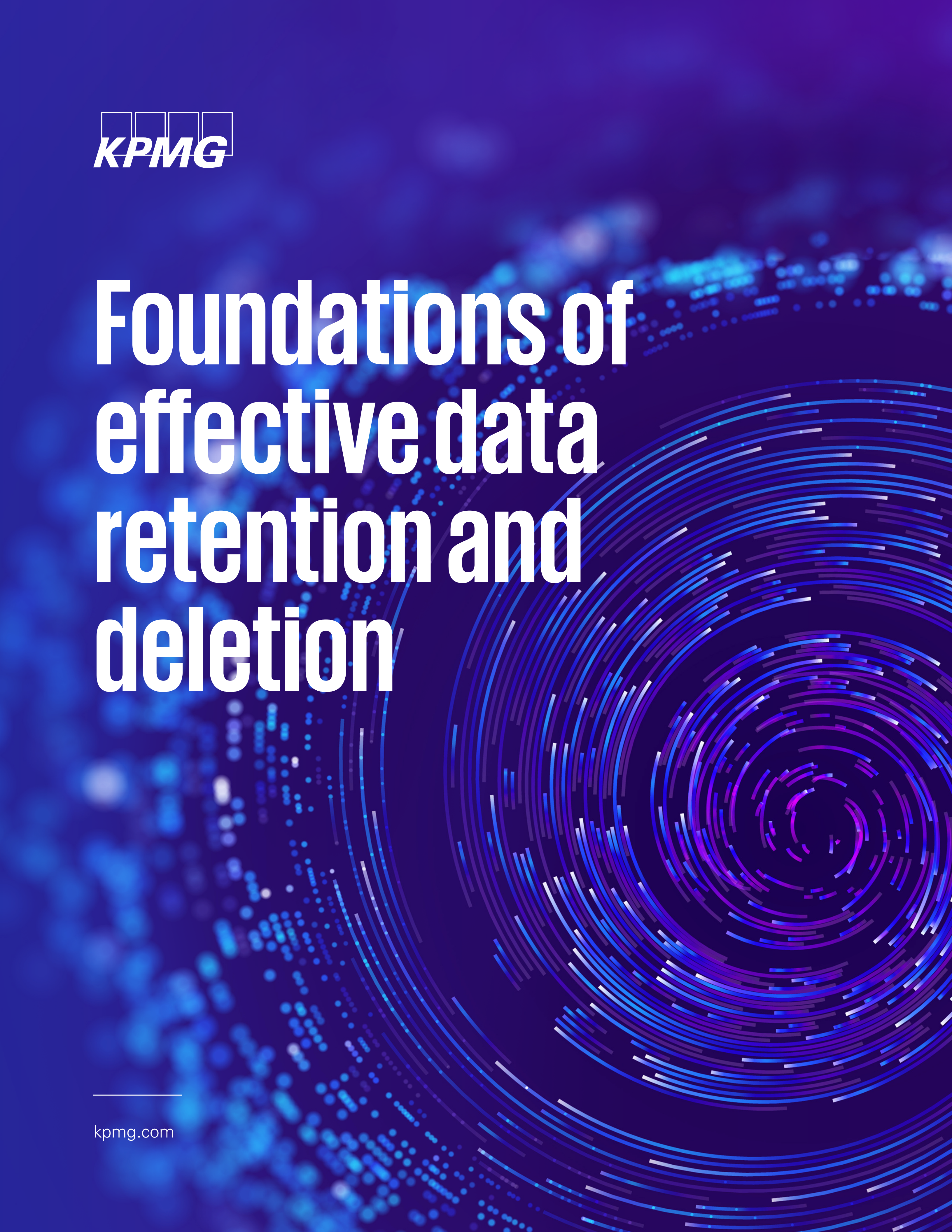


Foundations of effective data retention and deletion

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 must consider adopting retention and deletion leading practices, allowing businesses to harness the most value from their data, meet regulatory expectations, and maintain consumer trust.

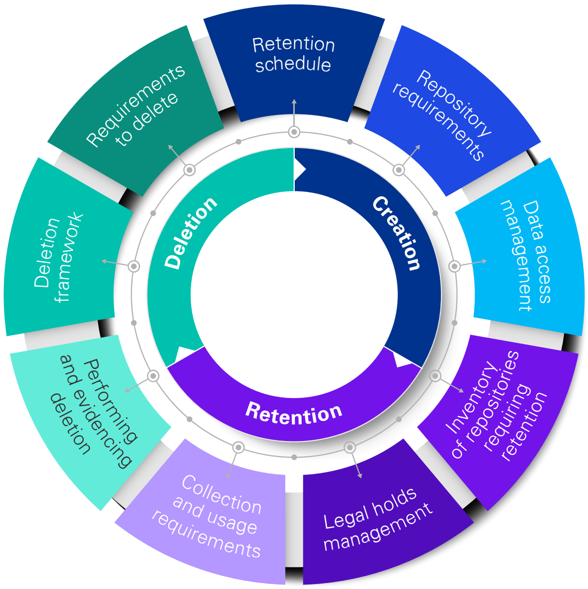
Balancing your data offense and data defense agendas

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, 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: Implement policies that define a structured approach to retention and deletion. By defining big-bucket retention classes that align with legal, regulatory, and business requirements, your organization is better enabled to retain your data for as long as it is required and dispose of data when it is no longer needed.

Repository requirements: Define requirements based on the content of the repository, at the point of repository creation and during any changes to what types of data a repository will store. For example, if the repository will contain records that have a data classification of highly sensitive, then the repository should be designed to segregate records from nonrecords, capture metadata necessary for deletion (i.e., capture triggers), and be deployed with access restrictions, etc. Additionally, when deletion may not be feasible or economical, consider archiving and masking in order to mitigate risks associated with over-retention.

Data access management: Incorporate retention and deletion requirements when defining data access controls. It is imperative that data that are records have their integrity maintained and are, therefore, only stored within a repository that is protected from unauthorized addition, deletion, alteration, use, or concealment.

Inventory of repositories requiring retention: Catalog your data storage locations with a data management platform, enabling you to demonstrate adherence to legal, regulatory, and business retention requirements. A data management platform facilitates data type classification, prioritizes retention protocols, and allows for retention requirements to be uniquely tailored to meet your organization's needs.

Legal holds management: Protect your organization from potential spoilation and unnecessary litigation risk with a legal hold management process that tracks legal holds from issue to release of the notice, as well as cataloging legal holds in your inventory of repositories requiring retention. As a result, data relevant to litigation matters, and other investigations, is preserved and deletion is suspended until matters are released.

Collection and usage requirements: Align your data retention and deletion processes with data privacy collection and usage requirements, so Personal Information (PI) is retained only for the purpose it is collected for, and its usage is restricted to its intended use.

Performing and evidencing deletion: Delete data securely and capture 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: Define a set of procedures and controls (e.g., approvals and other supporting documents) to guide the secure, defensible deletion of data in accordance with legal, regulatory, and business requirements.

Requirements to delete: Identify and document the criteria for mandating data deletion, such as PI 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 seamless 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.

Key benefits

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

Seamless 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

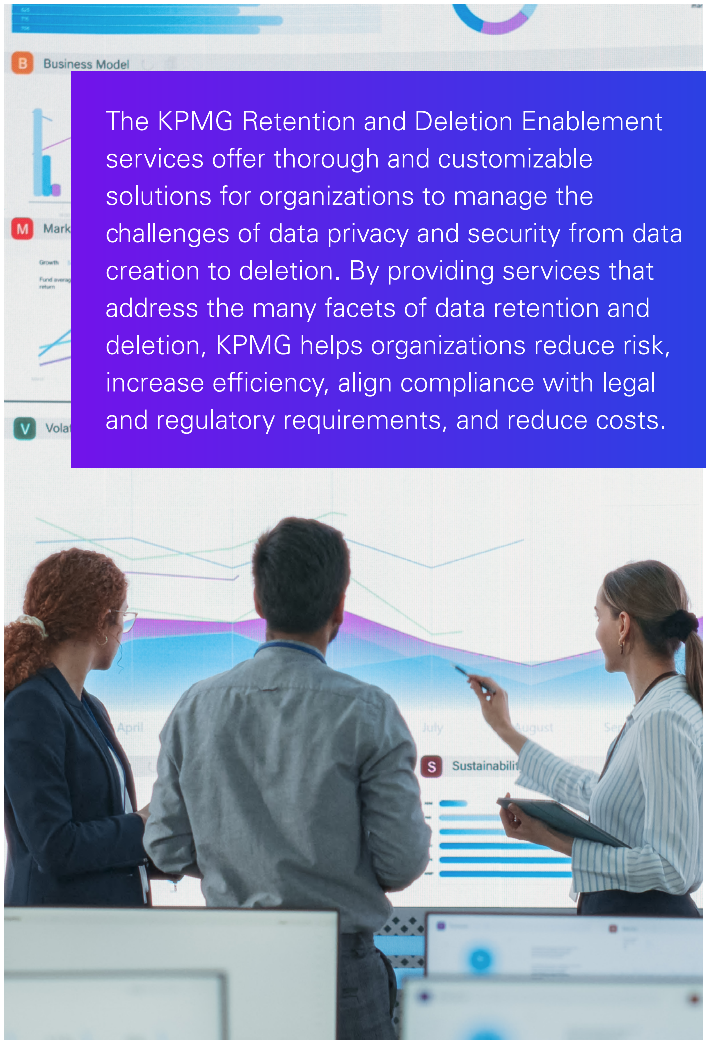
03 Use case development and requirements (including PI identification and remediation), tooling selection, and implementation

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

Orson Lucas
Principal, Cyber Security Services
KPMG LLP
704-502-1067
olucas@kpmg.com

Lee Merrill
Director, Cyber Security Services
KPMG LLP
904-354-5671
lmerrill@kpmg.com

Manoj Thareja
Director, Cyber Security Services
KPMG LLP
480-559-1586
mthareja@kpmg.com

Stephen Bartel
Director, Cyber Security Services
KPMG LLP
216-875-8038
sbartel@kpmg.com

Additional contributors: Ashley Ryan and Benjamin Bukai.

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**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

DASD-2024-15772