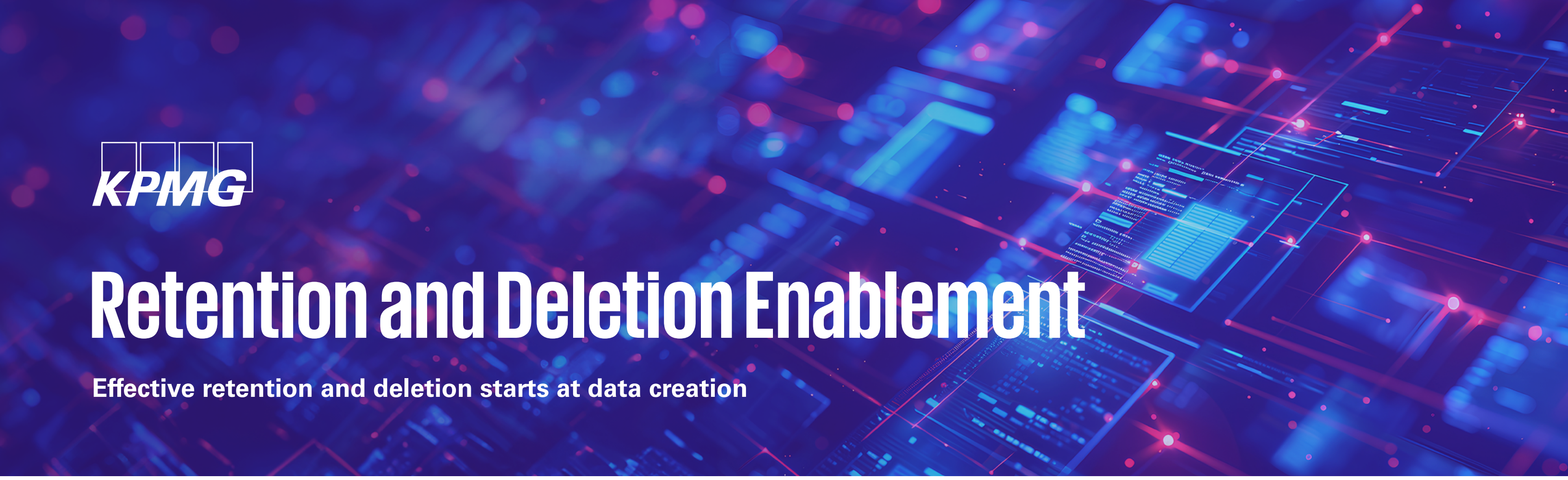


Retention and Deletion Enablement

Effective retention and deletion starts at data creation

Balancing your data offense and defense agendas

Maintaining a balance between your data offense and defense agendas is essential for effective data management. While a strong data offense can provide valuable insights and a competitive edge, failing to prioritize your data defense can expose your business to significant risks such as data breaches or legal and regulatory actions.

To strike a balanced data management strategy, consider the following:

01 Retention and deletion is central to data defense, organizations should not retain data that no longer has a business purpose or analytical value.

02 Putting too much emphasis on data defense can hinder business operations, decrease productivity, and result in missed opportunities.

03 Strive to strike the right balance between data offense and defense, so your business can leverage data proactively while safeguarding against internal and external threats.

Striking this balance will position your business to spur innovation, compete in a challenging marketplace, and drive profits while simultaneously protecting itself from potential threats posed by a complex, ever-evolving threat, regulatory and litigation landscape.

Benefits of effective data retention and deletion

Effective data retention and deletion practices offer a variety of benefits, such as:

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.

Cohesive 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 processes: 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, classified, 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.

How KPMG can help

Maturity assessment and roadmap

Function implementation and transformation

Use case development, requirements, tooling selection, and implementation

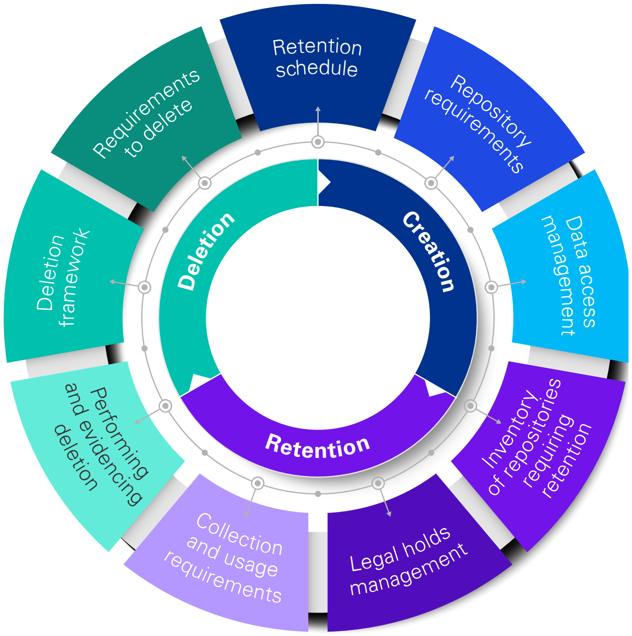
Regulatory response

Implementation of defensible disposition framework and associated process

Active support for legacy data disposition

Striking a balance—Implementing leading practices across the data lifecycle

Businesses should adopt leading practices across the data lifecycle—creation, retention, and deletion—in order to enable effective retention and deletion. At KPMG LLP (KPMG) our approach enables a balanced offense and defense through our Framework:



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 KPMG?

Our Retention and Deletion Enablement services offer comprehensive and customizable solutions for organizations to manage challenges arising from data creation through deletion. By providing tailored services that address different facets of data retention and deletion, KPMG helps organizations reduce risk, increase efficiency, address legal and regulatory requirements, and reduce costs.

Contact us

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

Lee Merrill
Director, Cybersecurity and Tech Risk
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, Cybersecurity and Tech Risk
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: in | **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.