KPMG

Data rich governance

Three keys to leading consumer data and information practices

kpmg.com

Companies rich in consumer personal data thrive on the power of data analysis to enhance the customer experience, streamline operations, and redefine markets. Although regulation wary, these companies face growing global and jurisdictional pressures to protect data security, privacy rights, law enforcement standards, and fair and reputable business operations. Evolving on the heels of directives such as the EU's General Data Protection Regulation (GDPR) and high-profile data breach and data sharing incidents, three keys to leading consumer data and information governance stand out. These include:

Developing consistency in processes

Operationalizing data and information governance compliance

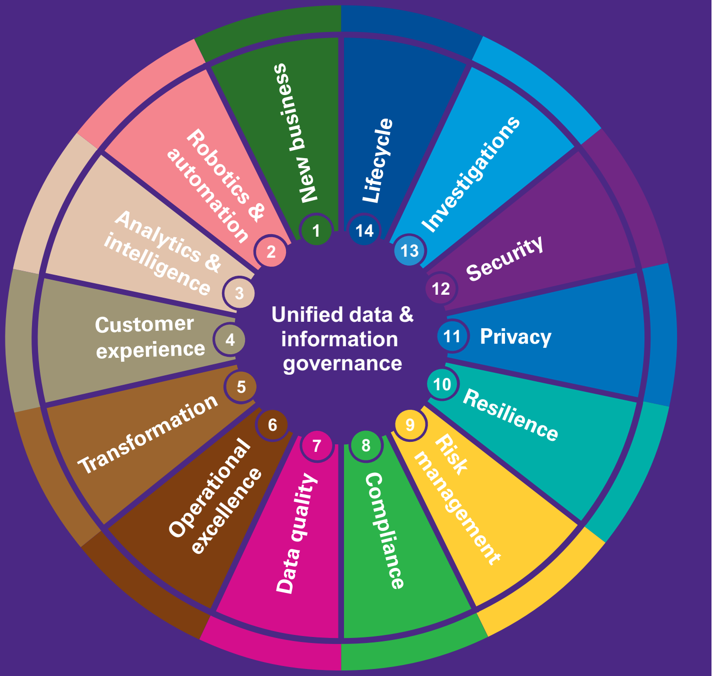
Implementing automation

Developing consistency in processes

A key principle in consumer data and information governance is developing consistency across global operations and centralizing compliance activities. Instead of managing data risk in siloes with little interconnectedness in scope and approach, leading organizations are linking their privacy programs across cybersecurity, information lifecycle management, legal hold, and eDiscovery. By connecting these key disciplines, organizations can see improvements in these areas and manage all major business and IT change initiatives with these disciplines in mind.

Evolving scope of governance: components of unified data and information governance

While data rich governance continues to evolve, it is comprised of many core components that drive unified data and information.



As part of their efforts to improve consistency, organizations must also examine their third-party relationships and their metrics and reporting processes. Enhanced third-party cooperation can improve general risk practices, including mitigating risks around the Foreign Corrupt Practices Act and other anti-corruption laws, while improved metrics and reporting processes can help both operational uses as well as executive decision-making.

Organizations should consider the following key actions in developing consistency in their processes:

- Link consumer privacy governance and accountability with other programs focused on security, information lifecycle, legal hold and discovery, cyber defense, and incident management
- Develop a framework and charter to require major change initiatives (new services, new products, new businesses, new territories, new on-premises platforms, new cloud providers, retirement of old systems) to account for major risk factors
- Identify and implement key policies and procedures as well as a formalized risk and control framework for third-party data management; obtain a level of comfort that data sharing is being conducted in accordance with an enterprise-wide privacy policy
- Develop enterprise-wide metrics to tie investment in consumer data privacy compliance to improving program maturity, and track these metrics as key KRIs/KPIs
- Implement culture change protocols so that all employees understand their responsibility when it comes to third-party data sharing and the risks it can pose; tie this to company-wide value statements
- Review contracts and user agreements to foster consistency and compliance with emerging issues such as breach notifications and data erasure requirements.

Operationalizing data and information governance compliance

Operationalizing unified data and information governance in new technologies can help companies improve their overall maturity. Tools such as data subject access requests, privacy by design, privacy impact assessments, incident management, and data processing can help avoid potential financial loss and sanctions; centralize and minimize their toolset; classify and track relevant assets; prioritize limited resources; improve teaming; and integrate with existing infrastructure. These tools can also help organizations capture and validate "good consumer personal data" and manage customer data preferences against using data to provide personalization through offers or customer reward programs.

Governance, Risk and Compliance (GRC) technologies can provide tools to assist in program management, risk management, audit management, and vendor risk management. New technologies can also help respond to incidents, manage threats and vulnerabilities, monitor security and incidents, remove customers as their profiles change, and identify customers that should be denied services due to fraudulent activity or other indicators. It can also help in encryption, anonymization, and masking and redaction. Some organizations are using tools to track business activities against supporting IT applications. Others are improving privacy programs with existing process-oriented tools as well as investment in privacy-focused and hosted applications, complaint inquiry, and notice and consent management.

Organizations should consider the following key actions when operationalizing data and information governance compliance:

- Embed unified data and information governance in new technologies to improve overall maturity.
- Evaluate GRC and/or process automation tools that can be leveraged and expanded to support privacy compliance
- Consider investing in process-oriented tools and privacy-focused and hosted applications, complaint inquiry, and notice and consent management.

Of those surveyed in KPMG's CEO Survey said protecting customer data was a priority.[1]

[1] Growing Pains: 2018 U.S. CEO Outlook, p.10.

Implementing automation

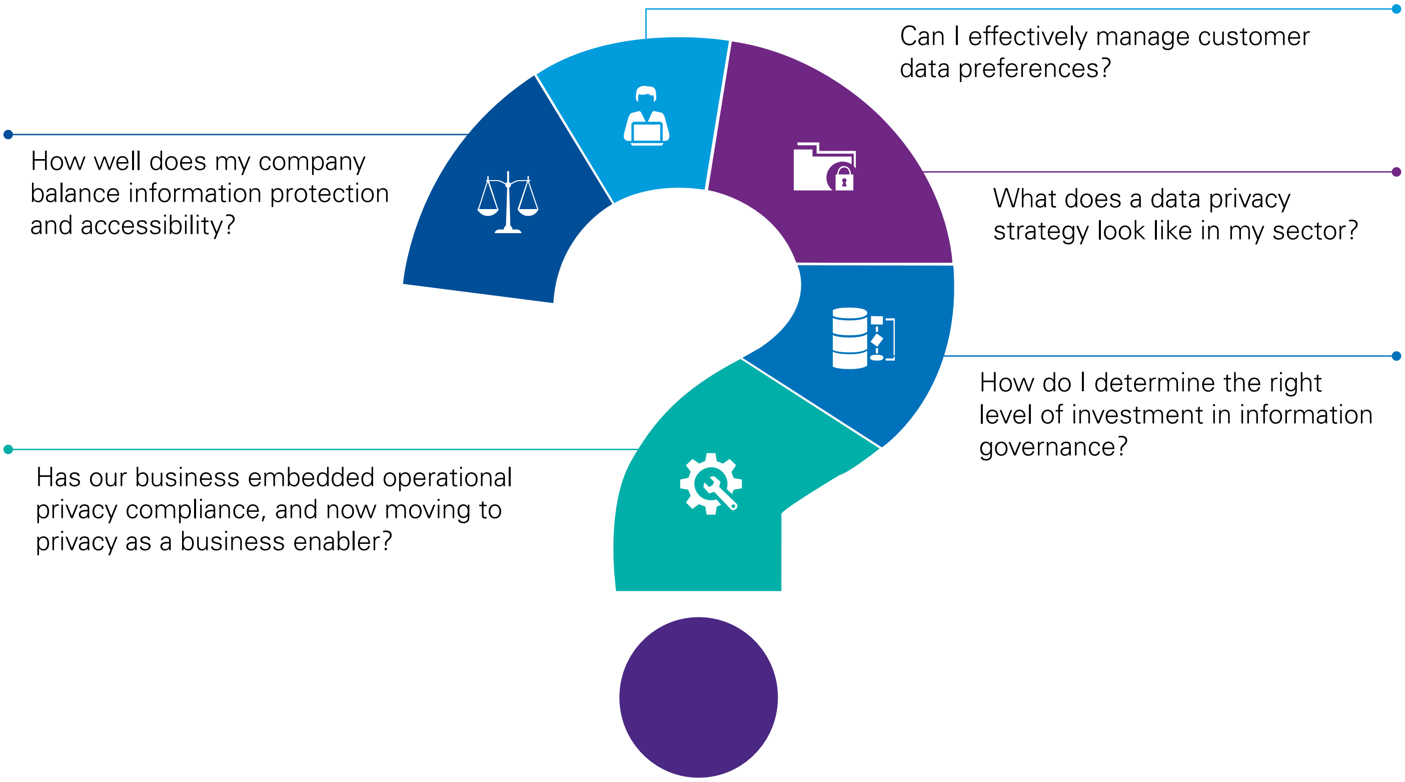
Processes embedding compliance (rather than built for compliance alone) enable companies to streamline operations and achieve desired outcomes. From data subject access and document fulfillment to user acceptance and contracting, embedding automated steps and controls helps simplify and enhance business and risk management activities. It can help monitor customer engagement and preferences as the organization combines internal data with other data sets.

Automation requires firms to first evaluate evolving technology against business considerations in the context of data and information governance. For example, organizations must begin to streamline and enforce consistency in entrenched processes. They should also manage convergence across business units as privacy compliance laws continue to evolve and strengthen as other jurisdictions, including U.S. states, consider consumer data privacy laws modeled after, or similar to, GDPR. Some organizations, for example, are evaluating discovery tools in attempts to automate data mapping. With this focus on simplifying and automating processes, firms can begin the transition to operating in a "business-as-usual" environment with improved maturity.

Organizations should consider the following key actions when automating processes:

- Evaluate technology against data and information governance business considerations
- Streamline and enforce consistency across data processes and business units
- Evaluate discovery tools for data mapping automation.

Key questions for data rich governance



How well does my company balance information protection and accessibility?

Can I effectively manage customer data preferences?

What does a data privacy strategy look like in my sector?

How do I determine the right level of investment in information governance?

Has our business embedded operational privacy compliance, and now moving to privacy as a business enabler?

Contact us

Amy Matsuo
Principal, Advisory
Regulatory and Compliance Transformation (R&CT), Solution Global and National Lead
Regulatory Insights, National Lead
T: 919-664-7302
E: amatsuo@kpmg.com

Steven Stein
Principal, Advisory
Privacy, Co-Leader
T: 312-665-3181
E: ssstein@kpmg.com

Duleep Rodrigo
Principal, Advisory
Risk Consulting, Consumer & Retail Industry Leader
T: 213-817-3150
E: drodrigo@kpmg.com

Michael S. Lamberth
Managing Director, Advisory
Operations & Compliance Risk
T: 804-241-2795
E: mlamberth@kpmg.com

Orson Lucas
Managing Director, Advisory
Privacy, Co-Leader
T: 813-301-2025
E: olucas@kpmg.com

Contributing authors

Amy Matsuo
Principal, Advisory

Steven Stein
Principal, Advisory

Swati Austin
Director, Advisory

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

kpmg.com/socialmedia