Data rich and regulation heavy

Navigating risk compliance in a data rich and heavily regulated landscape

Key highlights

Continue regulatory and policy focus

Regulatory and public scrutiny of personal data management continues to increase with the proliferation of data privacy and consumer protection laws across the globe. To keep up, organizations must take action to enhance their compliance programs and understand their overall data environment.

Increase data and security controls to address risk

Data privacy and security is a critical discipline for organizations. The volume and type of personal data collected by organizations influences its risk profile and can increase the number of resources needed to mitigate those risks. Organizations must maintain flexible and responsive data privacy and security programs that adapt to evolving threats and build customer trust.

Foster a culture of privacy

An organization that provides transparency and choice for its consumers around the use of their personal data has a competitive advantage. Trust has become a critical measure for consumers. The failure to recognize and respond to building a trusted strategy is a reputational risk that can easily result in public outrage, loss of consumers, and damage to an organization's brand.

1 Regulatory and policy focus

Rapid technological change and the digitalization of society has increased the amount of consumer data. The desire to move faster and be more customer oriented has made consumer data a more crucial resource to organizations. Businesses rich in data can leverage it to enhance customer insight, expand customer reach, personalize products and services, improve competitive position, and speed up technological innovation. To respond, regulators have advanced privacy policymaking at an unprecedented speed, attempting to keep pace with the rate of technological change and offer meaningful protection of consumer privacy in an increasingly digital society.

In the United States alone, a total of 60 data privacy bills were considered across 29 states in the 2022 legislative cycle[1]. The rate at which bills are being introduced is indicative of a widespread

[1]Privacy Matters in the United States, published by International Association of Privacy Professionals, 2023.

movement to better protect the consumer and their data across the US. Major legislative efforts have also been introduced across the globe. In 2022, the European Union (EU) passed two major laws: the Digital Markets Act and the Digital Services Act, both of which include data privacy requirements and are expected to significantly bolster the protections already provided by the General Data Protection Regulation (GDPR).

Other laws coming into force in 2023 include The Artificial Intelligence Act, The Data Act, and The Data Governance Act. Beyond the EU, regulatory change is occurring in the United Kingdom, Australia, Canada, India, and Hong Kong, among others.

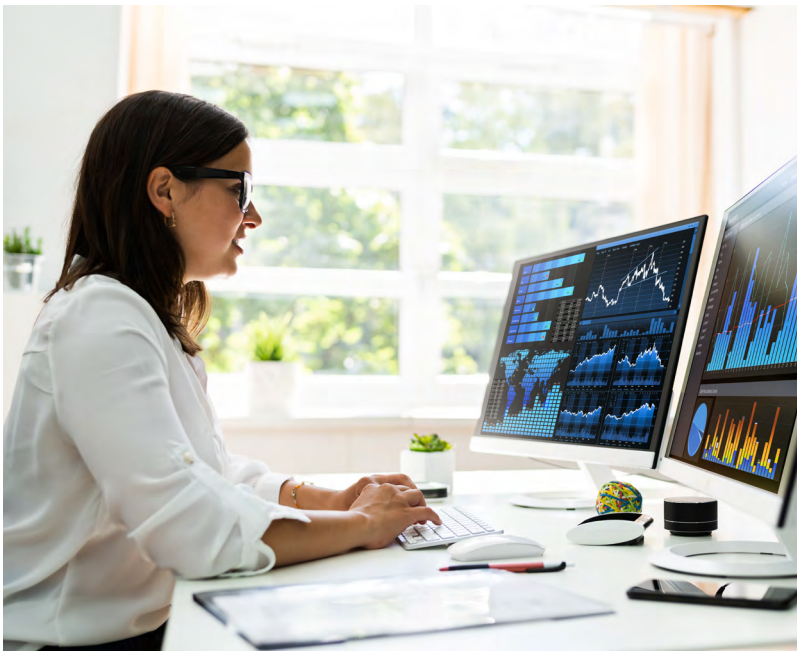
While the rate of regulatory change is undeniable, the approach to privacy lawmaking varies by jurisdiction. Some legislatures, such as the EU and California, have established themselves as the trailblazers of privacy law, passing proactive, progressive regulations that have persuaded other, more reactive legislators to take action (albeit often lighter-touch action). Differing approaches to lawmaking have resulted in a highly complex, and sometimes contradictory, legislative landscape for organizations. International as well as national organizations find themselves caught in a patchwork of laws they must carefully navigate without slipping through the cracks and falling into privacy purgatory. Even for the largest of organizations with generous compliance resource budgets, developing a privacy program that successfully ebbs and flows with the rugged tide of international and national privacy regulations is no small feat.

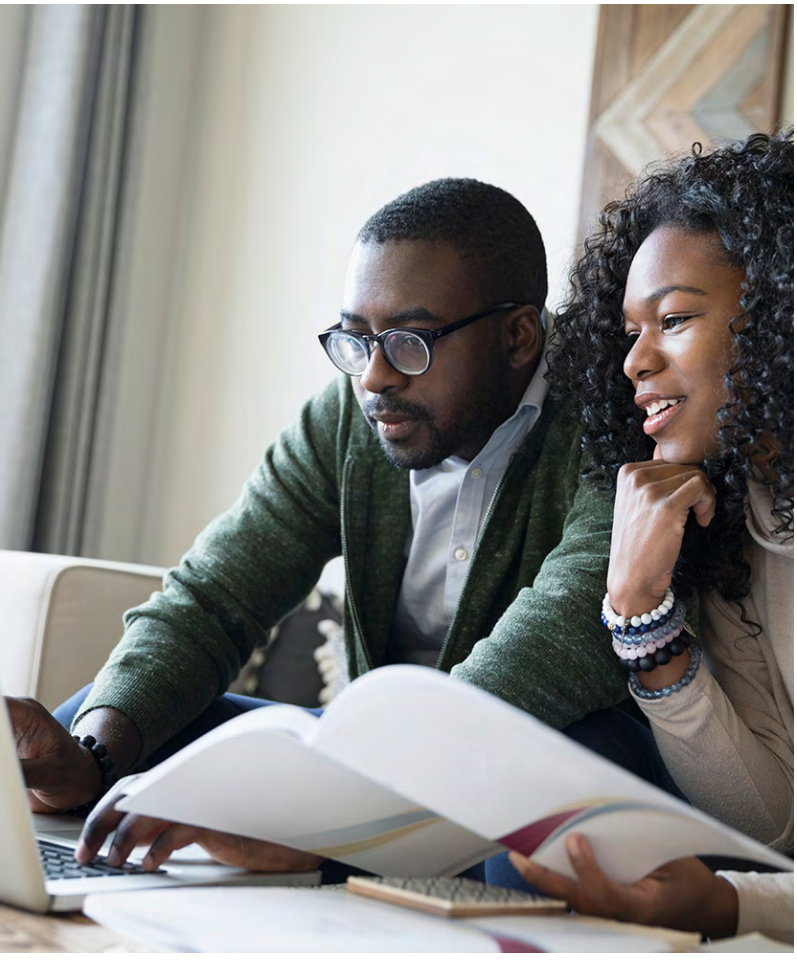
As a result of the regulatory boom in this area, treatment of personal data by organizations has come under hyperscrutiny, not only by supervisory authorities enforcing these new regulations, but also by the consumer, who has a heightened awareness of and ability to exercise their rights. It is important, therefore, that organizations possess strong knowledge of how they are managing privacy and security risk around consumer personal data and how they can go beyond mere protection of their brand. As the focus on these issues increases, stakeholders should be comfortable explaining how they assess their data security and privacy risks, the controls they have in place, and additional efforts they would recommend to further shore up their compliance programs to mitigate regulatory and reputational risks. In doing so, organizations can capitalize on the opportunity provided by the burgeoning privacy law landscape to showcase respect for privacy, build consumer trust, and differentiate themselves from their competitors.

This article discusses the issues that organizations should consider as they evaluate their existing risk management activities around data privacy and security and identify opportunities for enhancement.

2 Data privacy and security controls and risk

Propelled by the technological innovations and transformations of the Fourth Industrial Revolution and a dynamic regulatory landscape, strong data privacy and security controls are necessary. In addition to the sheer volume of personal data, the type, use cases, and data localization requirements are critical inputs for an organization to use to build controls to mitigate risk. Gone are the days where increased protection was only provided to Social Security numbers and financial data because many of the recent, privacy-focused regulations have expanded the definition of "personal data." These regulations require giving consumers more control over their personal data and how it is being used. The regulations also impose restrictions and establish governance around the sharing of personal data between the original recipient and any third-party organization. Together, these concerns contribute to an expansive risk profile.





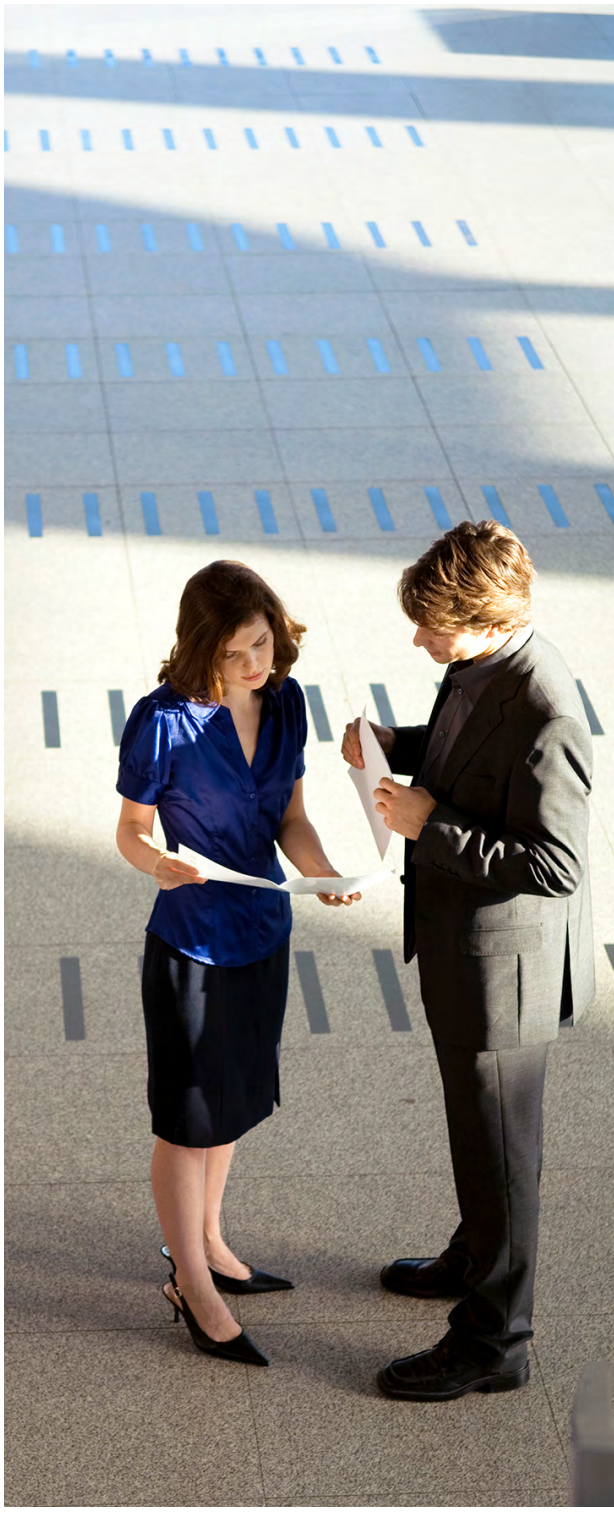
3 A culture of privacy

Consumer trust and an organization's reputation are critical to maintaining market share. In the KPMG 2022 Cyber Trust Insights, respondents from cybersecurity and privacy executive roles identified that improved profitability, better customer retention, and enhanced business reputation were all top benefits of increased consumer trust. However, consumer trust can be lost in an instant. Data spills, whether caused by internal mishandling or unauthorized access, are commonplace in news headlines. Those who build privacy and security cultures also know that organizations are struggling to respond to consumer requests because of a lack of visibility and understanding of their third-party ecosystem. When a customer requests access, deletion, or transfer of their data, there are processes that must be followed to receive, validate, and respond to these requests. Additionally, it is important that technology infrastructure is in place to enable this functionality. In other words, to what degree of confidence can an organization say, "here is all of the personal data we have about you"? Does your organization know the wide-ranging supply chain for that personal data and what risks the organization faces as a result?

4 Key actions

We have outlined a number of key actions an organization can take to begin mitigating these types of risks and concerns. First, to be effective, data privacy and security must be embedded into an organization from the top down. The goal is to start with the overall business strategy and buy-in from the board and C-suite and ask for a comprehensive regulatory compliance and risk management program that addresses privacy, security, and other key areas of risk. A team can advocate for the security and privacy portions of the program by considering the challenges presented by the company's operating model, identify accompanying risks, and flushing out how these risks and mitigating actions can shape the design, build, and operation of the company's products and services. There are other considerations as well:

- Be fastidious with your inventory of personal data (or Record of Processing Activities (RoPA)) to optimize visibility, understand purpose of personal data use, and monitor heavily scrutinized data types and processing activities (e.g., children's data, selling of data, and third-party data sharing).
- Establish a program for identifying, addressing, and managing compliance requirements.
- Conduct regular, holistic data privacy and security audit and impact assessments, aligning them with relevant laws and regulations as required.
- Build and grow an organizational approach to security and privacy risk management and regularly assess for opportunities to enhance.
- Use security-by-design, privacy-by-design, and privacy-by-default principles to embed key compliance requirements.
- Establish a control management framework to govern the design, implementation, and maintenance of controls used to address security and privacy risks.
- Conduct regular testing and monitoring of data privacy and security controls.
- Implement data stewardship standards, including roles, workflow, onboarding and training, and metrics.
- Evaluate and, where able, implement privacy-enhancing technologies to further technology innovation while strengthening the responsible use of personal data.



5 Key questions

- Do we effectively measure and report to the board of directors our risk mitigation activities related to our data privacy, compliance, and security controls?
- Do we have a robust data privacy and security risk assessment process?
- Does our compliance program include processes to track, ingest, and operationalize regulatory requirements?
- Are we using real-time and automated prevention and detection controls to alert us when we are near or exceeding risk tolerance levels for privacy, security, and reputational risks?
- Are we clear and concise in communicating with our customers what personal data is being collected, how it is being used, and how they can exercise their consumer rights?
- Does our comprehensive third-party oversight to include a clear understanding of how our customers' data is being used and adherence to contractual obligations?

KPMG is here to support the evaluation, strategy, and transformation of your compliance program as you navigate the advancing regulatory landscape. Grounded in three key tenets—visibility, protection, and trust—our Privacy service offerings can help you at any stage of your compliance journey:

- **Regulatory compliance support:** Bring in our Privacy subject matter professionals to perform maturity and readiness assessments, conduct gap analysis, and design program strategy across your applicable data protection landscape (e.g., the GDPR, US state laws, US sector laws, and in-country regulations).
- **Tactical privacy support:** We can provide recommendations on approach and assist with the implementation of core privacy processes, including data inventories, data mapping/records of processing activities, data subject rights fulfillment, and privacy/data protection impact assessments.
- **Automation and tech enablement support:** Our team of Privacy professionals and technologists can help you navigate complex issues and design a technology strategy that aligns to your business goals while supporting a positive end-user experience.

Interested in exploring further? Reach out to us.

Austyn McLoughlin
Managing Director
Cyber Security Services
415-963-8038
austynmcloughlin@kpmg.com

Anita Barksdale
Director
Cyber Security Services
713-319-3654
anitabarksdale@kpmg.com

John Kemler
Managing Director
Risk, Regulatory & Compliance
212-872-5852
jkemler@kpmg.com

Contributing authors

Rachael Reinis
Manager
Cyber Security Services

Clowance Wheeler-Ozanne
Senior Associate
Cyber Security Services

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

kpmg.com/socialmedia