Privacy compliance challenges

The pursuit to protect, manage, and govern data in a tumultuous regulatory landscape

KPMG's Compliance Briefing Series

June 2016

kpmg.com

Introduction

In the wake of the European Parliament's approval of the General Data Protection Regulation (GDPR) on April 14, 2016, and the European Court of Justice's (ECJ) decision in October 2015 to strike down the U.S.-EU Safe Harbor agreement governing cross-border transfers, many compliance leaders are struggling to interpret how those rulings and the proposed EU-U.S Privacy Shield (a new cross-border transfer framework entered into at a high level between the EU and U.S. Department of Commerce in February 2016) will impact their organization. While immediately taking action on the highest risk areas, compliance leads are simultaneously reevaluating their overall approach to privacy and compliance within their organizations, including roles and responsibilities, tools, risk assessments, and coordination across compliance, Information Technology (IT), legal, and internal audit functions.

This briefing document details how organizations are addressing privacy challenges in myriad ways. It includes insights from KPMG professionals' firsthand discussions with executives and their stakeholders, and provides key takeaways to help organizations bolster privacy compliance efforts.

Approach to privacy compliance

The ever-changing regulatory landscape of privacy requirements presents organizations with opportunities to refine their privacy programs. The maturity of each organization's privacy program may vary, depending upon their industry, size, and global presence. Arguably, the healthcare and financial services industries are some of the most heavily regulated, due in part to the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). Irrespective of industry, any organization that processes personally identifiable information (PII) must have policies, procedures, and controls in place throughout its enterprise. Organizations should be supported by the three lines of defense and align themselves with the regulatory requirements in the jurisdictions in which they operate in order to mitigate their risks of privacy breaches. As with other types of regulations, an organization's compliance approach must have, in part:

- Proper culture and governance in place to reinforce the messaging that privacy must be maintained and to address both internal and external breaches
- Education, training, and awareness efforts
- Privacy risk assessments
- Ongoing monitoring and testing of the privacy program, including monitoring and tracking of regulatory changes
- Reporting mechanisms to internal stakeholders as well as to external stakeholders on an as-needed basis, supported by predictive measures
- Incident management protocols to respond to privacy breaches, and with particular respect to crisis management.

Compliance's role in managing data privacy

Compliance leaders recognize that privacy risk from an enterprise-wide perspective can be significant and requires proper resourcing and coordination.

Many organizations have a designated chief privacy officer (CPO) who has oversight of the privacy program. Typically, this CPO sits within the centralized legal or compliance function, or to a

Leading practices relating to privacy compliance efforts include:

- Established governance and roles for managing data privacy (an integrated approach to privacy compliance)
- A clear understanding of current regulatory requirements with an eye on those forthcoming
- A holistic approach to managing internal and external risks.

KPMG

lesser extent within IT, and may even sit within risk management. In some instances, the Chief Compliance Officer (CCO) serves as the CPO. Largely based on the nature of where the CPO sits in the organization (legal or compliance), the most popular established reporting lines are to the CCO and/or the general counsel. Seemingly, when an organization's centralized privacy team is slimmer, the CPO role may be a part-time responsibility. For some organizations, the role of the CPO is relatively new, and they are still working to refine the reporting structure, roles, responsibilities, and coordination mechanisms.

Regardless of where the CPO resides in the organization, partnership, coordination, and communication with operational groups, as well as with compliance and legal, remain essential. This close coordination is particularly needed since privacy is often thought of as a blend of legal and compliance matters and because responsibilities for specific tasks impacting privacy are usually split. It is typical for legal to have responsibility for developing and revising privacy policies and for providing advisory guidance on an as-needed basis. IT, on the other hand, would have responsibility for safeguarding personal information in electronic format, with compliance serving primarily in an operations role. In some organizations, compliance departments have input into privacy training and have involvement in privacy communications. In addition, CPOs can be partners in addressing how to best maintain privacy with respect to social media and specifically with employees' personal communications therein.

One particular challenge for compliance leaders is understanding how to keep abreast and properly informed of all the regulatory changes in the privacy area on a global level and in a cost effective manner. In today's environment, this is a particular issue with the EU changes in privacy expectations and with concern about anticipated privacy development in the Asia-Pacific (ASPAC) region. (See page 4 for details on EU privacy law.)

The size of organizations' centralized privacy team appears to vary depending upon an organization's size, industry, risk exposure, and the maturity of their programs. In addition, organizations with global operations appear to favor small, centralized privacy teams with a larger network of supporting part-time "privacy compliance advocates" or "privacy compliance contacts" and legal advisers in local regions. A centralized approach globally helps organizations to address the divergence of domestic privacy regulations around the world and create visibility, while also enabling them to track and reconcile legal advice centrally. This is also thought to yield a more consistent approach.

Further, governance committees often are beneficial, providing additional reporting lines as well as a means to escalate and address privacy matters. In addition to governance committees, some organizations have privacy steering committees with representative members from some or all of the following: legal, IT/security, human resources, Internal Audit, compliance, and the business units. Compliance leaders believe an enterprise-wide committee helps engage members of their organization, including senior operational management, obtain their buy-in, and deter rogue activity.

The existing regulatory landscape

In the U.S., there is no one specific federal data protection law or regulation that sets forth data security standards for all organizations. Instead, there are various industry specific regulations issued at both the federal and state levels. This creates a "patchwork" of requirements that organizations must consider.

- The Privacy Act of 1974 (95 U.S.C. 552a)
- Department of Justice's guidance on the Privacy Act
- Financial Modernization Act of 1999 (GLBA standards)
- HIPAA
- Health Information Technology for Economic and Clinical Health Act and HIPAA omnibus final rule
- Federal Trade Commission (FTC) Act Section 5 notification laws and regulations

Sample U.S. regulators:

- Financial regulators
- Federal Communications Commission
- State attorneys general
- Department of Health and Human Services
- FTC

Global laws:

Europe

- The EU Data protection Act outlines provisions and conditions under which personal information can be transferred outside of the EU.
- Data Protection Directive – The existing regulatory regime in the EU, which dates back to 1995, provides a set of guiding data protection principles that member states must individually enforce. The Data Protection Directive is nonbinding for individuals.
- Member state laws – Country-specific legislation implementing the Data Protection Directive principles at the member state level. Member state laws are often inconsistent in the ways they implement the Data Protection Directive.
- General data protection regulations (GDPR)– Recently adopted data protection legislation across the EU that will be binding on all member states and provide standardization for how personal information can be processed and transferred. GDPR will become directly applicable in all Member States on May 25, 2018.[1]

Latin America

- Many Latin American countries recognize data protection and privacy in their constitutions. Some countries, like Colombia, Mexico, and Argentina, have taken more comprehensive stances on privacy by enacting laws that organization must comply with regardless of industry sector.

Asia Pacific (ASPAC)

- ASPAC countries have shifted to a regime similar to the EU. Many countries have enacted comprehensive data protection laws that govern cross-border data transfers. Russia recently enacted a data localization law that would require storage of any Russian citizen's personal data on servers based in Russia.

[1] European Parliament News, Brussels, Rikke Uldall (April 14, 2016)

FTC enforcement

In recent years, the FTC has brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile. In at least 47 cases since 2002,[2] the FTC has cited organizations for failing either to design or to implement an appropriately comprehensive privacy or data security program. Generally, the settlements outline standard parameters of a data security program, including the need to have an adequately trained chief data security or privacy officer and the need to conduct regular risk assessments. However, detailed guidance for what a privacy program should include are not specifically set forth by the FTC or any other U.S. regulator.

In a recent example from early December 2015, a worldwide financial organization settled allegations with the FTC that its poor data security practices exposed the payment card information of many consumers in a series of breaches. Although the organization will not pay a monetary fee for these breaches, it must "establish a comprehensive information security program designed to protect cardholder data as well as conduct annual information security audits, among other steps designed to safeguard consumer's information.[3]" The action further cements the data security authority of the FTC.

[2,3] IAPP, Portsmouth, NH, Patricia Bailin (September 19, 2014)

"What's really important is to make sure that there is dialogue, there are discussions, there's collaboration. So you have a concerted approach."
— Doron Rotman of KPMG LLP

Holding company challenges:
A holding company with subsidiaries brings particular challenges to privacy governance. For compliance leaders, there can be tension in deciding what level of escalation, oversight, and management the holding company will have versus the subsidiaries. The decision is often influenced by the name recognition of the holding company (greater name recognition may require more coordination and oversight at the holding company level), as well as the organization's culture, risk tolerance, tolerance for inconsistency, and the diversity of privacy risks across the subsidiaries.

When assessing what to centralize at an enterprise-wide level, compliance leaders also try to balance the enterprise need for consistency in approach with the subsidiaries' independence. For example, CCOs often may prefer to establish a centralized unit with proper expertise to obtain legal advice that can then be tracked and disseminated in a controlled, consistent manner to the subsidiaries with responsibility for drafting enterprise-wide privacy policies. However, other matters, such as specific types of privacy investigations or drafting of contracts that outline privacy responsibilities, may be handled exclusively by the subsidiaries, with regular enterprise-wide audits (to assess consistency with certain uniform requirements) or risk assessments. These controls would enable the holding company to maintain more of a consistent approach and to formally document reasons for exceptions or differences to the policy by subsidiaries based upon clearly articulated business imperatives and independent risks. In theory, such an approach can assist an organization in never being in a position where they are accused of having different policies or being inconsistent without having at least knowingly made an informed risk decision. Coordination between the subsidiaries and the holding company with respect to privacy matters is essential.

The tumultuous landscape: Safe Harbor disappears with a pending Privacy Shield as its replacement

Many organizations are greatly affected by the October Safe Harbor decision and its potential replacement, the EU-U.S. Privacy Shield framework. Some continue to evaluate what updates to their policies, procedures and processes are needed. They may have to revisit their privacy policies, assess their third-party contracts, and conduct internal assessments of their exposure to better understand their risks and prioritize their highest risk areas. Those who had executed model contracts with their subsidiaries and/or business partners that address data privacy and don't rely on the Safe Harbor are less impacted, but they may still be exposed due to the approaches of their third parties.

Privacy threats:

Organizations today face great challenges in protecting customer data and their intellectual property, such as research and development information, trade secrets, etc. Companies face internal threats from employees misusing or inappropriately using data, whether knowingly or not, as well as external threats commonly from privacy breaches or cybersecurity attacks. Third parties and subsidiaries seem to pose the greatest external risk. New technology, while beneficial to organizations, can also pose different risks. For example, social media is one such risk and where concerted coordinated approaches are being utilized for holistic risk management.

Breaking down the silos – The relationship between privacy and cybersecurity:

Conducting internet searches to identify privacy or privacy laws and regulations typically generate articles and information not only about privacy but also extensively about cybersecurity. This is because the two, privacy and cybersecurity, are intricately linked. Cybersecurity breaches frequently result in exposure of third-party data, implicating privacy concerns. This is clearly true when one considers the cybersecurity hacks of the U.S. Office of Personnel Management database, as well as hacks of consumer market companies, all of which exposed third-party names, addresses, and for some, credit card information.

Because of this linkage, some organizations have developed incident response protocols that they apply to both privacy and cybersecurity and are actively working to harmonize their approaches to both matters in furtherance of a consistent approach. As an example, compliance leaders may have one incident response plan and playbook for addressing incidents across the two focus areas which includes the following components:

EU privacy law may pave the way for new transatlantic pact

On April 14, 2016, the EU Parliament voted to formally adopt the the General Data Protection Regulation (GDPR). The decision ends nearly four years of legal discussions and will bring standardization to data protection across Europe.[4] GDRP will become nationally applicable in all EU Member States on May 25, 2018.[5]

Previously, on October 6, 2015 the EU's Court of Justice (ECJ) struck down the SAFE HARBOR. Thousands of companies had used this pact to transfer personal data of European customers to servers in the U.S. Such data includes social media profiles and payroll information.[6] While the ECJ order did not require an immediate end to data transfers, it did allow national regulators to investigate and suspend transfers if the organization involved does not provide "adequate protections."

It is estimated that at least 4,500 companies that store personal data relied upon the Safe Harbor framework to support their cross-border transfers.[7] After months of legal uncertainty, the EU and the U.S. Department of Commerce tentatively agreed on February 2, 2016 to a new framework for transatlantic data flows: the EU-U.S. Privacy Shield.[8] Actual requirements of the EU-U.S. Privacy Shield certification were released on February 29, 2016. It will impose stricter obligations on companies to protect data, limit government access to personal data for national security purposes, and provide several opportunities for European citizens to obtain redress in the event of misuse of their personal data.[9]

On February 24, 2016 President Obama signed into law the Judicial Redress Act, which extends the Privacy Act of 1974 to EU citizens, giving them standing to sue the U.S. government for privacy violations.[10]

While member states and organizations are officially on notice to begin preparation for implementing GDPR, the future of the Privacy Shield remains unclear. The Article 29 Working Party recently raised a number of objections to the proposed agreement, citing inconsistency with GDPR and a lack of clarity.[11]

The Privacy Shield is subject to final approval from the EU Commission and will undergo several committee reviews before that vote.

[4] European Parliament News, Brussels, Rikke Uldall (April 14, 2016)

[5] European Commission, Brussels (May 10, 2016)

[6] The EU introduced the Safe Harbor Privacy Principles in 2000, and the framework establishes seven points that organizations must adhere to, including: informing users of data collection, ensuring the security of the data, and offering the ability to opt out of data collection when using a service.

[7] The Wall Street Journal, New York City, Elizabeth Dwoskin and Robert McMillan (October 8, 2015)

[8] European Commission, Strasbourg, Christian Wigand (February 2, 2016)

[9] European Commission, Brussels, Melanie Voin (February 29, 2016)

[10] The White House, Washington DC (February 24, 2016)

[11] European Commission, Brussels (April 13, 2016)

– Initial assessments of risk and guidance for gathering information in the initial days to better determine who needs to be involved in responding to the breach and who needs to be part of the playbook response team

– Assignment of the team—which outlines who would be assigned to the team based upon set defined criteria. Teams are typically multifunctional and multidisciplinary.

Yet other organizations continue to view privacy and cyber security as separate and distinct compliance requirements and thus structure compliance for these in separate silos. Irrespective of the structure implemented, organizations recognize the importance of having a concerted approach to privacy and cybersecurity risks that is focused on dialogue, coordination and collaboration.

Privacy by design:

In an effort to holistically manage data risks and shift from a reactive to a proactive approach, some compliance leaders are focused on enhancing "privacy by design" efforts within their organizations. This means integrating privacy considerations up front into the design stage of a new IT system, product, and/or service offering. When organizations implement a "privacy by design" approach they develop tools and solutions early on to avoid a logjam over data privacy issues down the line. This proactive approach to assessing potential privacy risks helps organizations to avoid costly surprises and rework later on. According to KPMG LLP's (KPMG) Doron Rotman, regulators, and in particular European regulators, are increasingly messaging that organizations should have a "privacy by design" approach implemented.

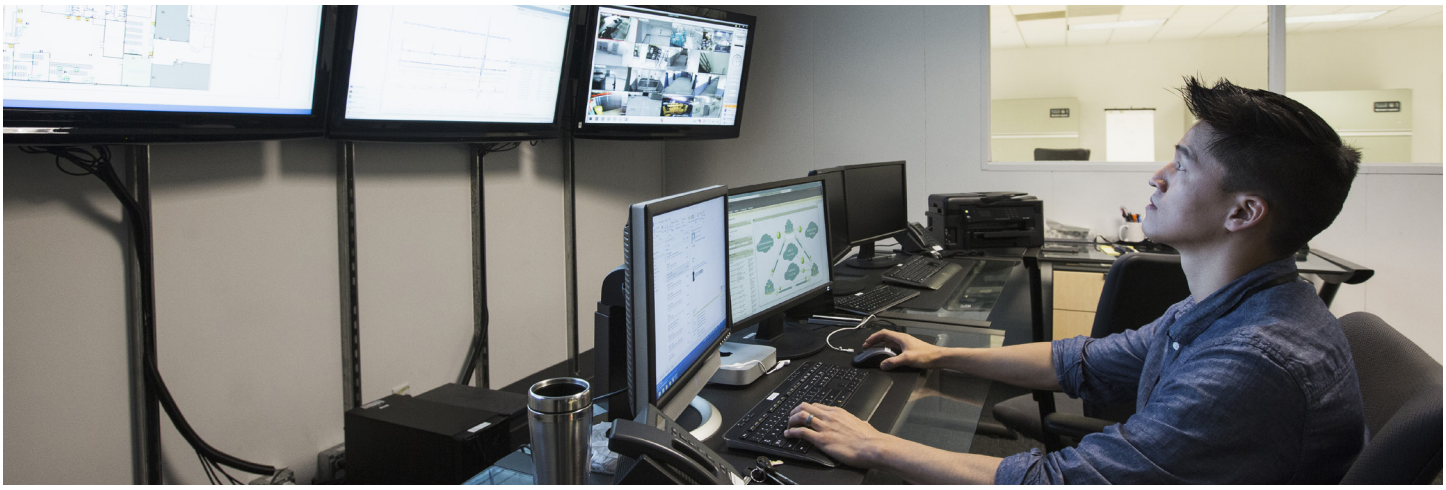
Organizations looking to implement a "privacy by design" approach may first want to proactively understand what data their employees are typically requesting for collection and for what reason. This can be accomplished by identifying a list of employees with roles and responsibilities that could implicate privacy concerns, perhaps through a retroactive review of prior data collection requests or through deployment of a short survey across the organization. Once an initial list is devised, it would be maintained and updated over time by the compliance department. As requests for data are escalated from additional employees, these employees would be added to the list. The organization would utilize the list to further socialize the concept of seeking input from compliance regarding data collection requests in advance and explain the compliance rationale for them. Additionally, organizations may opt to establish more governance over the process by creating a cross-functional committee (or adding to the responsibilities of an existing governance committee) to approve new data collection requests.

Privacy controls:

To mitigate privacy risks, compliance leaders are also focused on their internal control infrastructure and on assessing gaps and controls for enhancement. For example, leaders recognize the role that monitoring and auditing play in mitigating compliance risks and are working to further communicate and collaborate to achieve a more integrated approach across their three lines of defense. Priorities may include:

– "**Intelligence-Based model" monitoring** – organizations that utilize an intelligence-based model have moved toward coordinated and holistic monitoring across the enterprise of privacy risks (and potentially cybersecurity risks) in order to better manage internal and external threats. This model allows organizations to better understand, from multiple streams, what the attack parameters look like both internally and externally. Organizations that have implemented "intelligence-based" models are moving away from the simpler "guard-the-perimeter" model.

– **Automated monitoring tools** – organizations are increasingly utilizing behavioral type monitoring to identify internal privacy threats and risks. This type of monitoring seeks to identify abnormalities in employee behavior, such as inconsistencies with shift schedules, network log-ins at unexpected off hours, outbound e-mails, and accessing of certain Web sites, as well as typical red flags and strange data movements.



KPMG

- **Monitoring of privacy policy deviations** – organizations that have a global privacy policy may establish monitoring of variations to privacy policy as a control mechanism. In such instances, the policy would require a documented risk assessment when a variation is initially sought that addresses the business imperatives for the exception and which is maintained and updated on a regular basis throughout the year and continuously mapped to global policy. This requirement enables organizations to knowingly make an informed risk decision of exceptions, and compliance testing then is conducted to help ensure all exception requirements are properly granted and monitored by the applicable parties.
- **Audits of subsidiaries** – organizations regularly integrate privacy compliance into their audit plan. On a regular basis, audits can be conducted to help ensure adherence to global company-wide policy and local industry norms and to test that consistent implementation in cross-border transfers of private data are occurring.

Social media:

Compliance leaders are also focused and attuned to their evolving privacy risks associated with social media when employees might disclose private company information, insider trades, and IP. Additionally, it might also arise from employees that use company resources for personal social media posts. Many leaders seem to struggle with how to address employee use of social media. They seek to strike the right balance between employees' rights to personal expression on social media (and their entitlement to have a social media presence) with the organization's right to protect itself. Labor laws can also impact the restrictions an organization can place on employees' social media content. Many organizations find that their compliance controls and efforts in the privacy arena are evolving and a "moving target" as regulatory expectations evolve. Typical controls in the social media arena may include:

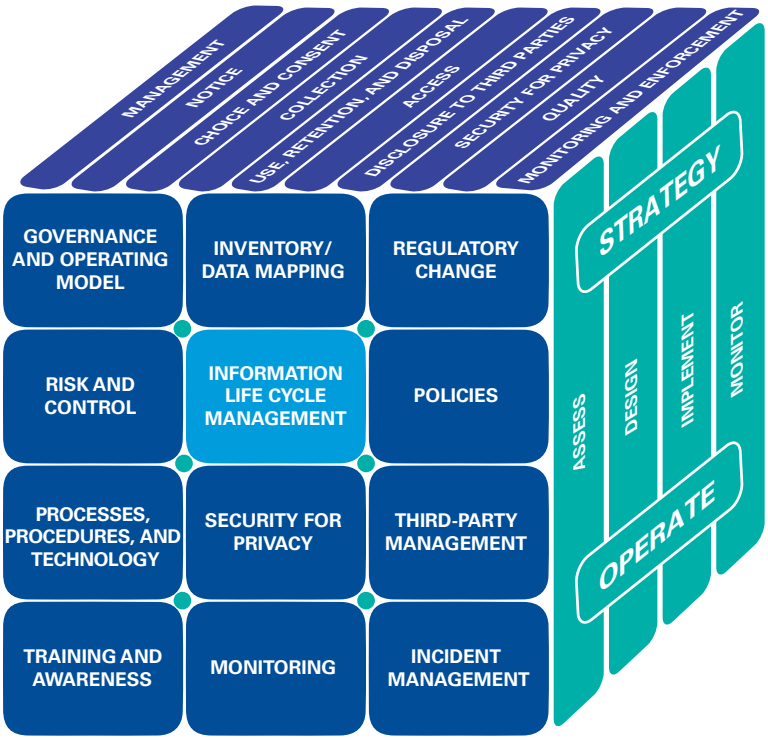
- Targeted trainings or communications that educate employees and explain social media policies, reminding individuals of their confidentiality obligations and that on social media they should be clear that they are only speaking on their own behalf and not on the organizations'
- Enhanced audits of departmental employees and their social media postings, a practice that is more prevalent in highly regulated industries
- For "volatile" issues, establishment of restrictions on employees sharing of their personal perspectives that can influence the market's perception of the organization and its brand.

Considerations checklist

- ✓ If not already in place, **encourage that a CPO be established in your organization, either in a full-time or part-time capacity.** If that role is separate from the compliance function, seek to establish strong communications with that individual to understand their responsibilities and how you can support and complement their efforts.
- ✓ Fully **understand the reporting and escalation structure** that is in place within your organization for privacy compliance matters.
- ✓ Build **collaboration between cybersecurity and privacy teams** within your organization by establishing communications and documenting processes.
- ✓ Work with the CPO or others who handle privacy responsibilities to **identify and document the types of privacy risks and develop a consistent approach to address and manage those risks,** including through third parties. It's also important to understand how those risks differ globally or among subsidiaries.
- ✓ **Develop awareness and training programs** to educate your organization's employee base on privacy policies, rules, and protocols.
- ✓ **Examine how the ECJ's invalidation of the U.S.- EU Safe Harbor framework affects your organization** and how the proposed EU-U.S. Privacy Shield certification requirements impact your confidence in your organization's potential risk exposure.
- ✓ **Establish a mechanism to monitor and track regulations** and key regulatory developments around privacy (e.g., anticipated development in the Asia-Pacific region).
- ✓ **Be sure** that processes are in place to **proactively address privacy risks as new products, services, or data requests** are initiated.
- ✓ Carefully consider the **privacy risks associated with social media** and develop protocols to mitigate those risks.

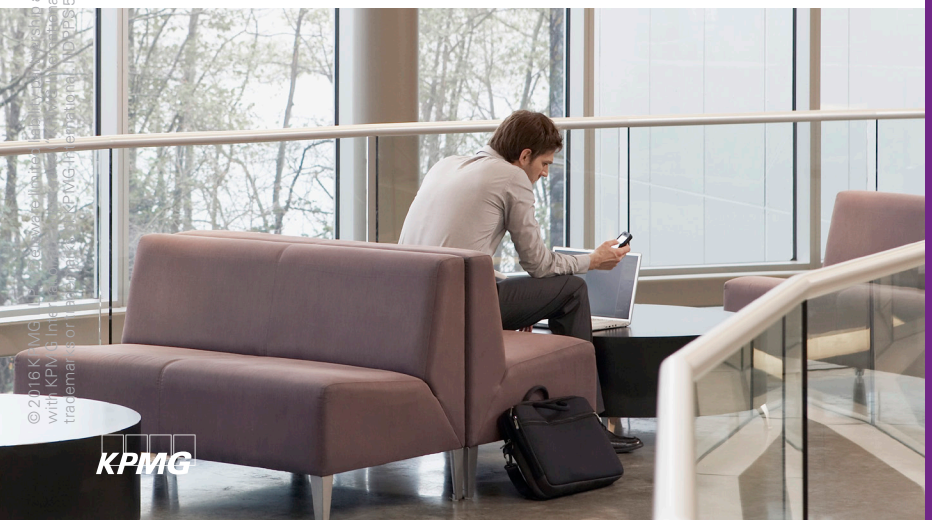
Privacy considerations: Balancing strategy and operations

To manage their privacy risks, organizations should implement risk-based approaches that are tailored to their individual privacy needs, risk appetite, and future business strategy. Compliance leaders can adopt a practical and pragmatic structure for organizing the day-to-day management and oversight required to manage privacy and compliance within their organization.



Key takeaways

- Good corporate governance and privacy risk management require integration and collaboration across compliance, legal, IT, HR, operations, business units and other functions.
- "Privacy by design" is a leading practice that enables organizations to proactively manage their privacy risks.
- To manage privacy risks, organizations need a robust understanding of their data flows and restrictions/protections for various data elements.
- Binding Corporate Rules and Model contracts are ways a company can comply with its cross-border data transfer requirements, but General Data Protection Regulation would still impose other compliance requirements not tied to data transfer
- A holistic approach to managing risks stemming from information breaches, internally and externally, can provide benefits. Such an approach may encompass privacy and cybersecurity; traditional monitoring and leading approaches, e.g., fusion centers; and behavioral monitoring.



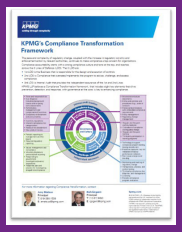
KPMG – Experienced in helping effectively manage privacy compliance

Our experienced professionals have supported hundreds of organizations—including highly complex, global enterprises – in meeting the increasing regulatory expectations for data privacy programs, including controls and security. Our services range from helping to reassess and retool the privacy mission and approach, governance and culture, as well as compliance business and risk operations. Ultimately, this can benefit organizations by:

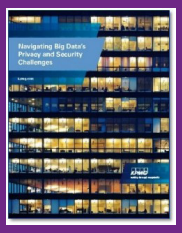
- Identifying and mitigating privacy risks, liability, and potential reputational damage
- Reducing costs and improving performance
- Increasing effectiveness and efficiency over the longer term
- Enhancing the organization's strategic business decision making.

KPMG perspectives

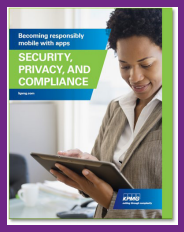
Our thought leaders publish regularly and here are just a few of our latest perspectives related to privacy compliance:



Compliance Transformation Framework. KPMG believes a compliance transformation framework, which includes eight key elements that drive prevention, detection, and response across the three lines of defense, with governance and culture at the core, is key to enhancing compliance.



Navigating Big Data's Privacy and Security Challenges. Discover in this white paper five key big data security and privacy challenges and seven areas of focus in KPMG's approach to help minimize risks and help maximize control over big data.



Becoming responsibly mobile with apps: Security, privacy, and compliance. Being "responsibly mobile" means embracing consumerization and business disruption while effectively managing risk through appropriately formulated and balanced mobile strategy, operations and delivery, and governance. These topics, along with key considerations for security, privacy, and compliance, are carefully examined within this paper.

Contact us

Privacy

Doron Rotman
National Privacy Service Leader
drotman@kpmg.com
408-367-7607

Compliance Transformation

Rich Girgenti
U.S. and Americas Leader for
KPMG Forensic Advisory Services
rgirgenti@kpmg.com
212-872-6953

Compliance Transformation

Amy Matsuo
KPMG's National Lead for
Regulatory Risk
amatsuo@kpmg.com
919-380-1509

Acknowledgements: Authored by Nicole Stryker. Content contributers: Christopher Kypreos and Karen Staines.

kpmg.com/socialmedia