KPMG

Data rich and regulation wary

Improving risk compliance in today's data rich environment

kpmg.com

Key highlights

1 Expect regulatory and policy focus

Personal consumer data abounds, and regulatory and public scrutiny of data management is increasing. Organizations must take actions to enhance enterprise risk controls, monitoring and overall data programs.

2 Increase data and security controls

Data privacy and security is an increasingly critical discipline for organizations, as data sharing, data access, and data protection risks and requirements evolve. Companies should embed data privacy and security programs throughout their organization and implement policies, procedures, and controls to manage and protect data maintained across the enterprise and held by third parties.

3 Drive individual consumer data and brand protections

The lack of authorization for, or transparency in, data sharing could cause a customer, public, or regulatory backlash and damage a firm's brand and reputation. Organizations must drive a culture and associated business practices that demonstrate consumer choice and protection, privacy and regulatory compliance, and partner and third-party accountability and stewardship.

Regulatory and policy focus

Today, consumer personal data is a valuable asset for many organizations, particularly as entities rich in data look for innovation in technologies to extend their customer reach and improve their competitive position. And in the current social media and technology environment, where consumers are willing to "share" so much about themselves, consumer personal data is more bountiful than ever before. However, as recent events demonstrate, consumers do not look kindly upon breaches in data privacy or misuses by organizations they trust, and brand and reputational risks from such breaches or misuses can result in extensive losses.

Regulatory scrutiny of data privacy, security, and consumer transparency is gaining steam, a trend likely to continue. The associated regulatory enforcement is likewise anticipated to increase. For example, the U.S. Federal Trade Commission (FTC) has recently reiterated its commitment to protecting customer privacy, hinting publicly at the possibility of enforcement actions when regulated organizations violate the EU-US Privacy Shield,[1] the FTC Act's Section 5 prohibition against Unfair or Deceptive Acts or Practices (UDAP),[2] or FTC orders on privacy and data security requirements.[3] In addition, the advent of the EU's General Data Protection Regulation (GDPR), scheduled to go into effect this May 2018, is already impacting the way organizations that touch any EU consumers manage data.[4] The GDPR is also spurring similar types of legislation in other regions and jurisdictions.

Against this regulatory and social backdrop, organizations need to better understand how they are managing privacy and security risks around consumer personal data and protecting their brand from reputational risks. This includes consideration of unintended exposure of user data, identity theft, and other legal restrictions. As the focus on this issue 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 in order to further shore up their compliance programs and mitigate regulatory and reputational risks.

This article discusses the issues that organizations should consider as they evaluate their existing risk management activities around data privacy and security and identify priorities to enhance further.

[1] Under the Privacy Shield, organizations in the EU and the US that voluntarily self-certify and commit to comply with the Privacy Shield Framework agree to comply with data protection requirements when transferring personal data between the EU and the United States.

[2] FTC Act Section 5 prohibits all persons engaged in commerce from "unfair or deceptive acts or practices in or affecting commerce."

[3] The FTC can take enforcement action when a company's data privacy and security practices violate the Section 5 prohibition against "unfair and deceptive acts and practices" or other federal laws.

[4] The EU's General Data Protection Regulation (GDPR), will affect U.S. firms, as it imposes EU data protection, along with significant fines, to non-EU organizations that use data from EU residents.

KPMG

KPMG's data risk management model

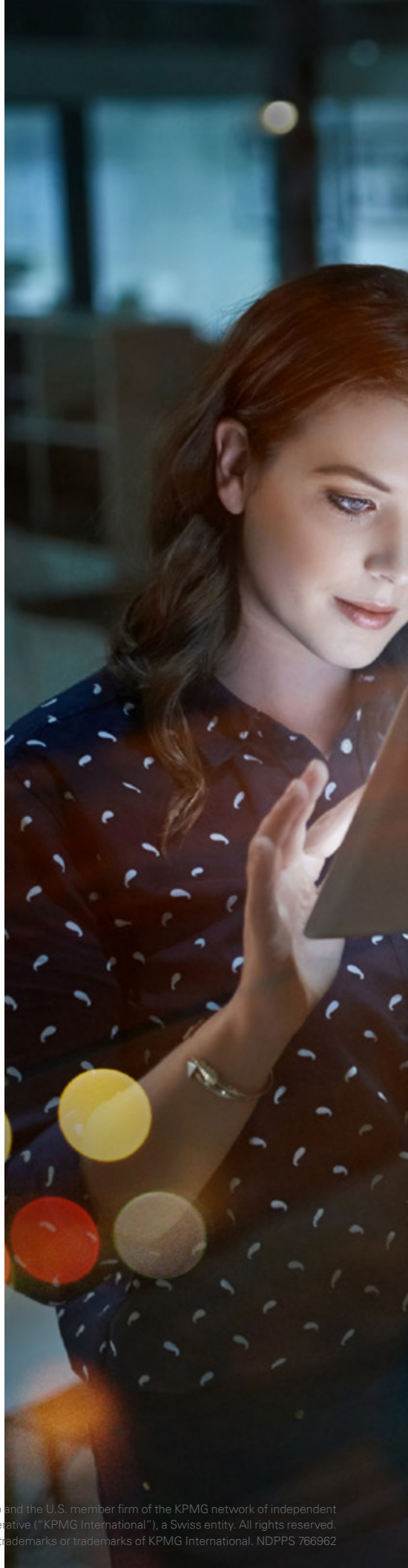
Data privacy and security

Data privacy and security is an increasingly critical discipline for organizations, as data sharing, data access, and data protection requirements evolve. Organizations face a number of constantly evolving risks around consumer personal data that could impact their operating models, including an expanded definition of personal data, strengthened privacy rights, new privacy compliance control and reporting requirements, and the potential for large fines and penalties. Additionally, the complex legal and regulatory landscape requires organizations to have robust, effective data privacy and security programs with appropriate policies, procedures, and controls to manage and protect data both across the enterprise and held by third parties with which your organization has a relationship.

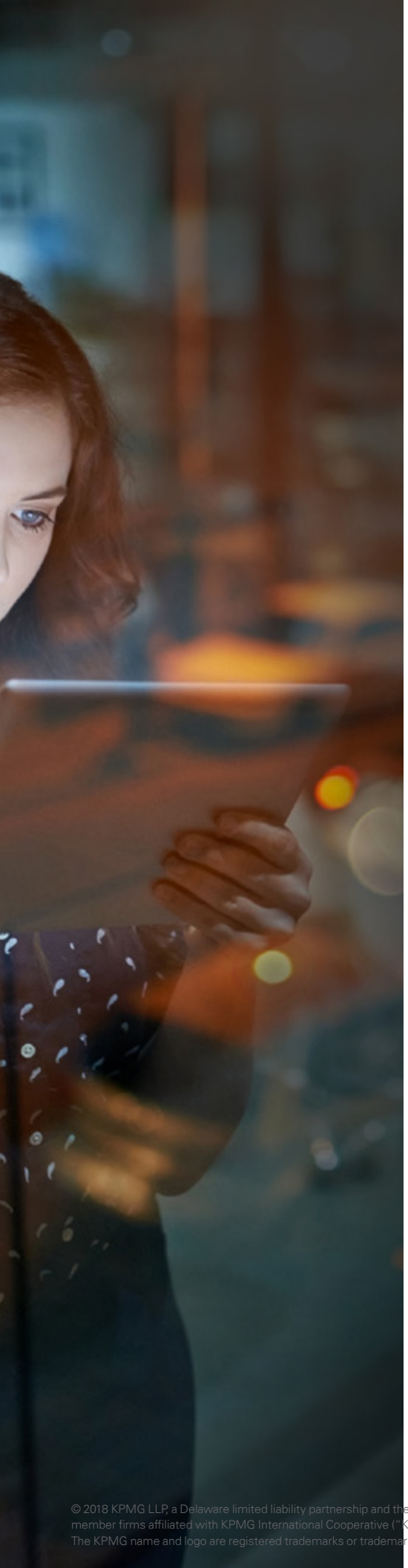
To mitigate these risks, data privacy and security must be embedded into an organization's business strategy, operating model, enterprise risk management programs, IT decisions, processes, and compliance program. It must also be embedded in how the organization conceives, designs, builds, and operates products and services. This can be a challenge for organizations, particularly those that are de-centralized or siloed.

Key actions

- Inventory the personal data that the organization collects, processes, stores, and shares
- Conduct a holistic data privacy and security audit and impact assessment
- Perform root-cause analysis on prior known inappropriate data sharing
- Assess compliance with privacy regulations, privacy notice and consent requirements, and contract provisions
- Assess data lineage governance, application programing interface (API) environment, and data obfuscation, encryption, and protection
- Identify at-risk business processes and data and develop an approach to mitigate these risks
- Evaluate third-party data usage, including identifying the third parties, how data is shared with them, and how that data is used; refine third-party data protocols to align with the Board's risk tolerance
- Evaluate and strengthen identity and access management, and implement privileged access controls and role-based access controls
- Establish and operationalize data privacy governance channels
- Implement a system to monitor data and alert management about data issues
- Evaluate and implement enhanced technologies (e.g., artificial intelligence, blockchain, behavioral analytics) to help prevent and detect data usage and access anomalies and/or unauthorized data sharing
- Implement a strong privacy governance program that is aligned with business strategy.



KPMG



Customer and reputational risk

Customer trust and an organization's reputation are critical to maintaining market share. A data breach, unauthorized or improper data sharing, or a lack of transparency in how data is shared could bring not only fines and compliance orders but also a backlash from customers, the public, or regulatory authorities that could damage a firm's reputation.

To mitigate these risks, organizations must implement robust regulatory compliance and enterprise risk management programs that also provide partner and third-party accountability and stewardship. Organizations must also drive a culture and implement business practices that demonstrate consumer choice and protection, and privacy and regulatory compliance.

Key actions

- Revisit ability of customers to opt-in or opt-out of data sharing, as appropriate
- Inventory related laws and regulations
- Evaluate regulatory and contractual obligations and requirements
- Implement data mapping capabilities that can identify all data records that relate to individual customers
- Assess risk management structure and measurement against consumer protections
- Use security-by-design and privacy-by-design principles to embed the compliance framework within the innovation processes to prevent data privacy abuses, reputational risk, and improve customer experience
- Establish and operationalize nonfinancial risk management frameworks, including data analytics/modeling and reporting
- Implement a program of timely customer communications on data issues
- Evaluate partners and third parties against the strategic plan for data sharing
- Implement third-party data stewardship standards, including roles, workflow, on-boarding and training, and metrics
- Evaluate and implement enhanced technologies (e.g., artificial intelligence, blockchain, behavioral analytics) to help prevent and detect anomalies in personal data sharing, onboarding, monitoring or surveillance of partners and third parties, and analysis, escalation, and resolution of customer confusion and complaints
- Implement data lifecycle management capabilities that support individual rights, such as data deletion and data portability.

Key questions

- Do we have a robust data privacy and security risk assessment process for our data exchange channels that results in a demonstrable challenge to onboarding, off-boarding, and ongoing monitoring and oversight?
- 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, consumer protection, and reputational risks?
- Are we clear and concise in communicating with our customers what of their personal data is being collected and how it is being used?
- Is enough information provided for a consumer to make an informed decision about how they choose to share their data?
- Are our terms of service clear and understandable by the average consumer, and do consumers have the ability to opt in or out of how their data is being used?
- Do our third-party and partner agreements contain formal, clearly defined and documented guidelines, procedures, and protocols on upfront and on-going due diligence, including any potential engagement in illegal activity or other misconduct?
- Do we need to re-evaluate risks in certain categories of third-party counterparts, such as political vendors or others?
- Does our third-party oversight include a clear understanding of how our customer's data is being leveraged?
- Do we have controls in place to ascertain if our third parties are adhering to contractual obligations?
- Do we effectively measure and report to the Board of Directors our risk mitigation activities related to our data privacy, compliance, and security controls?

KPMG

KPMG's client success stories

Case study

Data breach and data governance and controls

Client concern:
The client needed to determine the individuals who may have been impacted by a data breach and assess the associated program and controls around data security.

KPMG approach:
KPMG provided the client with a team that included security, data analytics, and privacy specialists to work alongside the organization's incident response/breach response investigators to analyze the data housed and transferred through the affected network and systems.

Outcome:
KPMG performed a root-cause analysis of the data breach, conducted a privacy and security assessment, and analyzed the data systems to determine additional individuals affected. KPMG also provided a process and governance map to operationalize data privacy governance channels and streamline similar operations for future incidents. Additionally, KPMG helped ensure business continuity by freeing up client resources so they may return to their daily activities.

Case study

Third-party data management

Client concern:
The client used third parties to deliver services and needed to understand how those third parties manage risks, including data privacy, on their behalf. With an exponential increase in the amount of data that is shared between companies and the complexity of the ecosystems for service delivery, outsourcing an activity did not absolve the client from the responsibility to manage the risk.

KPMG approach:
KPMG worked with the client to design a third-party risk management program (TPRM) that governs risk management across the product lifecycle. This included design of the initial due diligence activities prior to contracting; the design of a key control to prevent executing third-party contracts before completing the due diligence and developing an exceptions process whereby a contract can be executed without all due diligence being performed; processes for the ongoing management, including monitoring and assessing controls in place at the third parties; and termination of the third-party relationship.

Outcome:
KPMG assisted the client to design the TPRM program to help manage the intersection of privacy, information management, and third parties. KPMG used a set of gating questions at the outset and clarified the roles and responsibilities for the assessment and management of the risks through the lifecycle of the third-party relationship. KPMG also developed an alert system that included investigation and escalation processes as well as root cause analysis and trend reporting.

Contact us

Thomas Lamoureux
Principal Advisory
Industry Lead, Technology, Media and Telecommunications (TMT)
T: +1 206-913-4146
E: tlamoureux@kpmg.com

Amy Matsuo
Principal, Advisory
Regulatory and Compliance Transformation, Solution Global and National Lead
Regulatory Insights, National Lead
T: +1 919-664-7302
E: amatsuo@kpmg.com

Vijay Jajoo
Principal Advisory
Data Privacy and Security
T: +1 415-963-8698
E: vjajoo@kpmg.com

Guido Van Drunen
Principal, Advisory
Regulatory and Compliance Transformation, TMT Lead
T: +1 408-367-7592
E: gvandrunen@kpmg.com

Doron Rotman
Advisory Managing Director
Data Privacy and Security
T: +1 408-367-7607
E: drotman@kpmg.com

Contributing authors:

Amy Matsuo, Santosh Haranth, Swati Austin, Eric Kuhrman, Deepak Mathur, Nicole Stryker, and Phil MacFarlane

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

kpmg.com/socialmedia