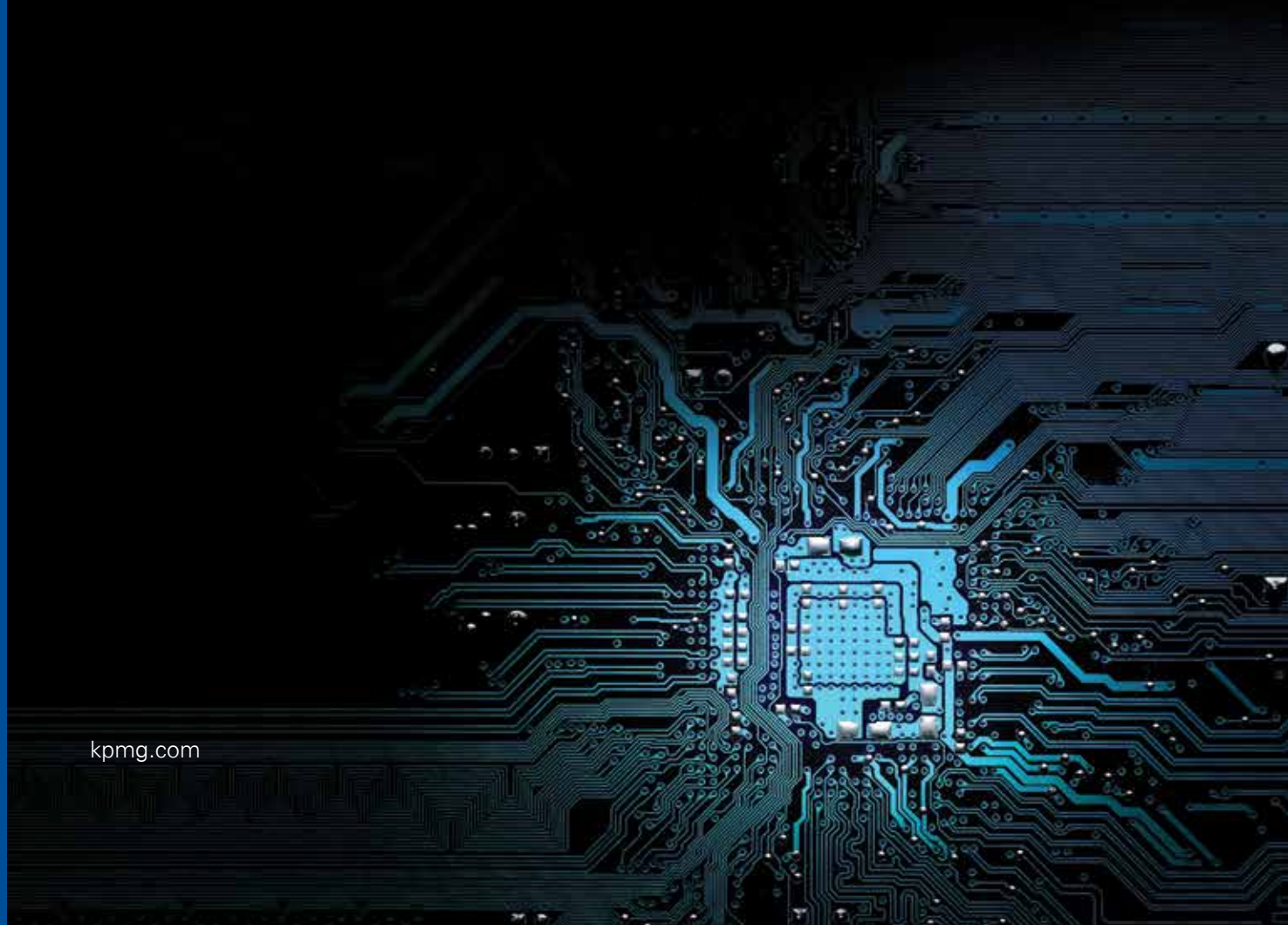
KPMG

Point of view

Converging U.S. and E.U. data protection requirements



kpmg.com

Executive Summary

Compliance implications for U.S. entities subject to the data privacy standards imposed by the E.U.'s General Data Protection Regulation

Because data breaches can have a severe impact on harmed organizations and individuals, cybersecurity and the protection of consumer data are a regulatory priority.[1] However, only 40 percent of the participants in KPMG's 2017 survey of U.S. Chief Executive Officers indicate they are well-prepared for a cybersecurity threat.[2] A second KPMG survey found integrating cybersecurity and data privacy compliance to be a top challenge for U.S. Chief Compliance Officers.[3]

Rapid technological developments and globalization have led to an increase in cross-border sharing of consumers' personal data, expanding data security risks commensurately. For the digital economy to develop across nations, a coherent data protection framework and consistent enforcement are needed to create a basis of trust. Recognizing this, the European Union (E.U.) Parliament adopted new standards in April 2016 for the protection of individuals in the European Union (generally referred to as "data subjects"). These standards, referred to collectively as the General Data Protection Regulation (GDPR),[4] will take effect in May 2018 and impact multinational organizations doing business in and with E.U. countries.

Compared to existing data protection regimes, GDPR expands the definition of personal data, creates new privacy compliance requirements, imposes large fines and penalties for violations of an individual's privacy rights, and applies an extraterritorial reach that subjects organizations based outside of the E.U., including U.S.-based organizations, to the jurisdiction of the European Union. There is no grace period once GDPR takes effect and U.S.-based organizations must prepare now in order to avoid the risk of country-level data protection authority inquiry, private-party litigation, significant fines (up to 4 percent of global revenue), or other penalties associated with violations of GDPR by the organization or its vendors.

In short, GDPR significantly increases the legal, financial, and reputational risks associated with the handling of personal data. It also provides an opportunity for organizations to design and embed privacy into emerging technologies in order to lower the cost of compliance, lower the cost of control, and increase consumer confidence.

KPMG

Overview of GDPR

Once effective, GDPR will replace the Data Protection Directive 95/46/EC. GDPR is an extensive regulation, creating numerous obligations for cross-border transfers of the personal data of individuals within the European Union. Key features and requirements of the new regulation include:

- An expanded definition of "personal data" to include any information related to a natural person that can be used *directly* or *indirectly* to identify the person.
  - Examples include name, photo, email address, social media posts, medical information, biometric data, or a computer IP address.
- An explicit emphasis on the principle of accountability. Under GDPR, organizations must put in place governance requirements that demonstrate how the institution complies with GDPR requirements.[5]
  - The appointment of a Data Protection Officer is required if the organization engages in "large scale" systematic monitoring or processing of sensitive personal data.
  - The organization must also have a local representative within any E.U. member state(s) where it does business.
- The requirement for an existing and documented lawful basis for processing personal data, such as pursuant to the data subject's consent or acting in performance of a contract. These bases are enumerated, and the particular basis used determines the subject's rights on managing the data.
  - Parental consent is required to process the personal data of children under the age of 16 for online services.
- New obligations for the organization and strengthened individual rights, including the:
  - Right to be Informed – Organizations must provide privacy notices to individuals. These notice requirements are consistent with existing privacy notice requirements.[6]
  - Right of Access – Individuals have the right to obtain confirmation as to whether their personal data is being processed and, if this is the case, they have the right to access that personal data and additional information, including to whom the data has been disclosed.[7]
  - Right of Rectification – Organizations must typically respond within a month to a data subject's requests to rectify inaccurate or incomplete data and to inform third parties of the rectification.[8]
  - Right to Erasure ("Right to be Forgotten") – Individuals have the right to obtain the erasure of personal data and to prevent further processing of that data in specific circumstances.[9]
  - Right to Restrict Processing – If individuals trigger the right to block the processing of personal data, an organization may store the data but may process it only with the data subject's consent or for limited purposes, including the exercise or defense of legal claims, and to protect the rights of another person or entity.[10]

- Right to Data Portability – Individuals have the right to obtain their personal data from an organization and to have it transferred between organizations. In certain circumstances, the organization must provide the requested personal data in a machine-readable format, such as a CSV file, free of charge and typically within one month of a request.[11]
- Right to Object – Unless an organization can demonstrate countervailing legal or other compelling claims, it must stop processing an individual's personal data for the purpose of exercising official authority, direct marketing, or scientific research. The organization must also give individuals the ability to object online.[12]
- Rights in Automated Decisions – In certain situations, GDPR enables individuals to forego automated decisions using collected data and seek human intervention instead. GDPR also requires organizations to deploy accurate sufficient controls when using automated processing methods to develop an individual's profile, which analyze performance at work, economic situation, health, personal preferences, reliability, behavior, location, or movements.[13]

— Enhanced data breach response plans, including deadlines to notify supervisory authorities and individuals affected by the breach within 72 hours. Failing to provide timely notices can result in fines up to 10 million euros or 2 percent of global turnover.[14]

— Permissible data transfers outside of the E.U. only if certain conditions are met, such as with an individual's informed consent, where required for the performance of a contract or where it is necessary for public interest.[15]

These requirements are broader and less specific than nearly all current U.S. requirements. As such, U.S. companies must be able to identify applicable GDPR requirements, which data subjects they apply to, and how internal processes and procedures need to be adapted to comply with GDPR requirements.

Many of our clients are focusing their energy and investment on the following "fundamentals":

— Privacy Governance Model

— Data Privacy Impact Assessments

— Record of Processing Activities

— Data Subject Rights

— Incident Response and Communications

Penalties

Under GDPR, an organization will be liable to private-party litigation for GDPR violations resulting from the actions of the organization, cloud data vendor, or other third-party providers.[16] Organizations need to be aware of their own GDPR risks, as well as those of any of their third-party providers.

Organizations in noncompliance with GDPR face stiff penalties. GDPR provides for a tiered approach to fines depending on the nature and severity of the infraction.

— For violations of Articles 8, 11, 25–39, 41(4), 42, and 43, administrative fines can be up to 10 million euros or up to **2 percent of gross revenue** (i.e., the total worldwide annual turnover) for the preceding year, whichever is higher.[17]

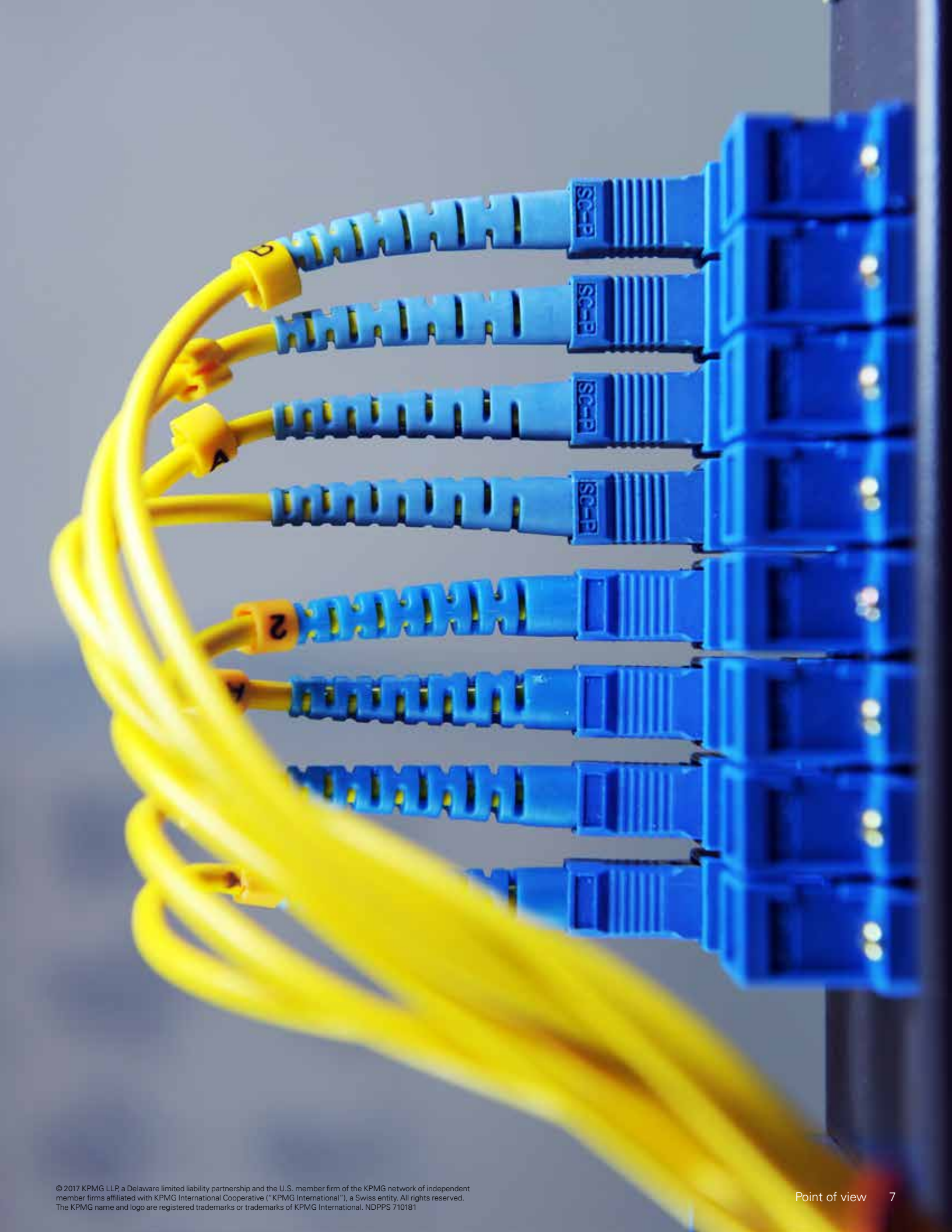
  These Articles generally address provisions related to consent for a child; processing data that does not require identification of the data subject; obligations of the organization, including general obligations, data security, impact assessments, and the data protection officer; and code of conduct monitoring and certification.

— For violations of Articles, 5–7, 9, 12–22, 44–49, among others, organizations are subject to administrative fines of up to 20 million euros or up to **4 percent of gross revenue** of the preceding financial year, whichever is higher.[18]

  These Articles generally address provisions related to the principles for processing personal data, consent, rights of the data subject, and transfers of personal data to countries outside of the E.U. or international organizations.

Clearly, noncompliance or violations of GDPR pose a substantial financial risk to organizations. The real question is not how much it costs to be compliant with GDPR but how much it will cost to ignore it.

KPMG



Industry Challenges/ KPMG Solutions

Organizations are faced with a multitude of challenges when evaluating GDPR. The first step is to evaluate whether the organization processes or holds the information of any data subject in the European Union. Once that is confirmed, the work begins to ensure compliance.

KPMG's Privacy Methodology establishes the information life cycle as the basis for effective Privacy controls in an organization, aiming to identify and manage the risks associated with personal information from its creation through to disposal.

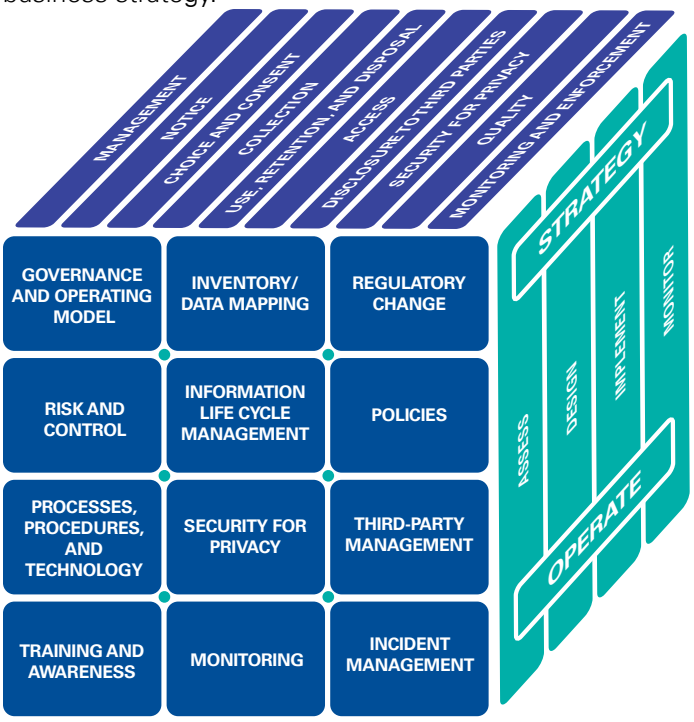
Compliance Transformation Framework

Compliance programs must be assessed and enhanced in response to new privacy regulations, such as GDPR. Key considerations include evaluating the organizational structure to appoint a Data Protection Officer, developing and updating a centralized inventory of privacy obligations and mapping them to policies and procedures, reviewing vendor relationships, completing risks and control assessments, conducting compliance testing, and developing compliance training and reporting requirements.

Privacy Management Framework and Transformation Cube

Our framework had been used successfully to help identify, define, and manage what is required in executing Privacy compliance programs and running day-to-day Privacy operations. Accelerators used in conjunction with the framework include a Privacy law repository, multijurisdictional Privacy controls gap analysis, and Privacy Impact Assessment tool.

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.



KPMG

Key Client Challenges and KPMG Solutions

Governance and Accountability

Organizations are struggling to demonstrate or produce evidence of the effective execution of key data governance processes and controls. Using KPMG's frameworks, organizations are able to more readily navigate their governance and operating models to consider changes that will holistically allow management of a privacy program.

— Does your organization have the right people with the right skill sets throughout the three lines of defense?

— Are your policies and procedures prescribing clear roles and responsibilities across the three lines of defense?

Production and Maintenance of Records

Complex global organizations are struggling with creating a consolidated, holistic view of personal data flows for data subjects and personal data and often have multitudes of interconnecting, siloed, and legacy systems without accountable owners. KPMG's information life cycle management and our approach to inventory and data mapping allow clients to consistently manage data flows and proactively address issues that may arise.

— Does your organization know and understand where all of the personal data of the data subject resides throughout your organization?

— Is your organization able to distinguish between covered and noncovered data subjects?

— Are your systems ready for opt-in versus active consent?

— Do your security protocols provide for quick identification and isolation of affected data?

Strengthened Individual Privacy Rights

Organizations are struggling to keep pace with increased demands from data subjects and often lack up-to-date consent documentation to demonstrate and assert legitimate interest provisions. KPMG's regulatory change management process allows organizations to implement and consider relevant changes to new and existing requirements to keep abreast of relevant privacy provisions.

Looking ahead

As organizations look toward the May 2018 compliance date, it is also important to prepare a road map for the continued optimization of GDPR capabilities. The following summarizes high-level considerations for future-state privacy compliance ambitions:

— 2017: GDPR readiness discussions as well as resource alignment and establishment of the project management office; design, build, implementation, and governance of privacy compliance "fundamentals"

— 2018: Continued rollout and extension of data mapping, data protection impact assessment, and data subject rights capabilities; introduction and fine-tuning of privacy technologies

— 2019: Compliance process and control convergence across business units and suppliers as privacy compliance laws continue to evolve and strengthen.

[1] Source: KPMG, Ten Key Regulatory Challenges Facing the Financial Services Industry, KPMG Americas Financial Services Regulatory Center of Excellence, available at https://home.kpmg.com/us/en/home/insights/2016/12/ten-key-regulatory-challenges-facing-the-financial-services-industry.html.

[2] Source: KPMG, Disrupt and Grow: U.S. CEO Outlook 2017, page 25, available at https://assets.kpmg.com/content/dam/kpmg/us/pdf/2017/06/us-ceo-outlook-survey-2017.pdf.

[3] Source: KPMG, The Compliance Journey: Summary of KPMG's CCO Survey Results, 2017, page 10, available at https://advisory.kpmg.us/risk-consulting/compliance-transformation/kpmg-chief-compliance-officer-survey.html.

[4] Source: General Data Protection Regulation (GDPR), E.U. Regulation 2016/679, April 27, 2016, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[5] Article 5 and Recital 39.

[6] Articles 12–14 and Recitals 58–62.

[7] Articles 12 and 15 and Recital 63.

[8] Articles 12, 16, and 19.

[9] Articles 17 and 19, and Recitals 65 and 66.

[10] Articles 18 and 19, and Recitals 67.

[11] Articles 12 and 20, and Recital 68.

[12] Articles 12 and 21, and Recitals 69 and 70.

[13] Articles 4(4), 9 and 22, and Recitals 71 and 72.

[14] Articles 33, 35, and 83, and Recital 85, 87, and 88.

[15] Chapter V, Articles 44–50.

[16] Article 82.

[17] Article 83.

[18] Article 83.

KPMG

Contact us

Amy Matsuo
Principal and National Lead
Regulatory Insights
T: 919-380-1509
E: amatsuo@kpmg.com

David Remick
Partner and U.S. Lead
Privacy Services Network
T: 404-222-3138
E: jremick@kpmg.com

Contributing authors

Amy Matsuo
Principal and National Lead
Regulatory Insights

David Remick
Partner and U.S. Lead
Privacy Services Network

Stephen Bartel
Director
Regulatory Risk Advisory

Karen Staines
Director
Center for Financial Regulatory Insight

Warren Mager
Manager
Regulatory Risk Advisory

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

kpmg.com/socialmedia