Through deeper insights into data collection, storage, and management, organizations can more effectively protect data in a risk-informed manner. KPMG privacy enablers help your organization automate key components of your privacy program and maximize the value of your existing ServiceNow investment.

Across industries, organizations struggle to have a consolidated and holistic view of data. They often find themselves with multitudes of siloed legacy systems, without accountable owners or even insight into the type of data that is being stored on these systems. This leads to a lack of visibility of sensitive data, posing tremendous compliance and reputational risks to the business.

In order to leverage privacy as a competitive advantage, organizations must establish a cohesive privacy and security strategy, appropriately enabled by the right underlying technologies.

The KPMG automated data privacy offering uses native ServiceNow capabilities to create a tech-enabled data privacy program. Our integrated approach to data privacy will help your organization gain an accurate understanding of the data used by applications, devices, business processes and third-party organizations. This increased visibility allows you to more effectively protect data with a goal of increasing customer trust.

## Privacy challenges addressed by KPMG privacy enablers

- Lack of a unified methodology to address new and changing regulatory requirements
- Inability to provide customers with control over the use of their data
- Data siloed across different technologies
- Limited integration between data privacy and broader cyber security and enterprise risk management needs
- Insufficient visibility into the management of sensitive data
- Lack of insight into third party organizations with access to sensitive customer data

## Visibility enables protection and trust

**Data protection**

**Visibility**

**Trust**

How would you run your company differently if you had accurate visibility into what data your applications and business processes use?
The KPMG automated data privacy offering using ServiceNow

KPMG privacy enablers save cost and time, while helping to maximize your existing ServiceNow investment. We leverage established data sets to build a foundation and then develop a customized platform of accelerators to meet your organization’s unique needs. The following represents existing application, content, and custom-connection privacy-based enablers:

Application enablers

- Privacy impact assessments (PIA)
- Privacy breach response
- Data subject requests (DSR)
- Data protection impact assessments (DPIA)
- PII self-attestations
- Business unit privacy assessments
- Business process privacy assessments
- Data analytics privacy reviews

Custom connections

- Data discovery tool APIs (e.g., Dataguise)
- OneTrust data mapping custom API

Content packs

- Privacy regulatory content (e.g., CCPA and GDPR)

KPMG offering provides:

- **Discovery**: A technology-enabled active discovery capability.
- **Mapping**: Linking discovered data to assets, business processes, owners, and third parties to create a complete understanding of the record of processing activities.
- **Risk and control rationalization**: Continuous rationalization of regulatory requirements with internal policies and controls.
- **Remediation**: Robust workflow capabilities for assessment and issues management.
- **Customer control**: User-led controls for data management.
- **Communication aids**: Clear and accessible privacy policies and notices along with thorough reporting.
- **Governance**: Ability to integrate with broader GRC processes, including third-party management, internal audit, compliance, and risk management.
- **Classification**: Assets reflect the sensitivity of the data stored on the device.
- **Coordination**: A powerful orchestration engine to drive coordination of the privacy technology ecosystem.
- **Integration**: Ability to integrate and consume data from point solutions.
- **Access control**: Limited user access to data and workflows according to organizational access requirements

Why KPMG

KPMG brings a distinct combination of technological experience, deep business and industry knowledge, and creative professionals who are passionate about helping you protect and build your business. We offer a global, multidisciplinary view of cyber and privacy risk, helping you carry privacy and security throughout your entire organization.

For more information the KPMG automated data privacy offering, please click here.

Contact us

- **Orson Lucas**
  Principal, Cyber Security Services
  olucaas@kpmg.com
- **Prasanna Govindankutty**
  Principal, Cyber Security Services
  pkgovindankutty@kpmg.com
- **Christopher Kaleyias**
  Director, Cyber Security Services
  ckleleyias@kpmg.com

www.kpmg.com/us/cyber

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.