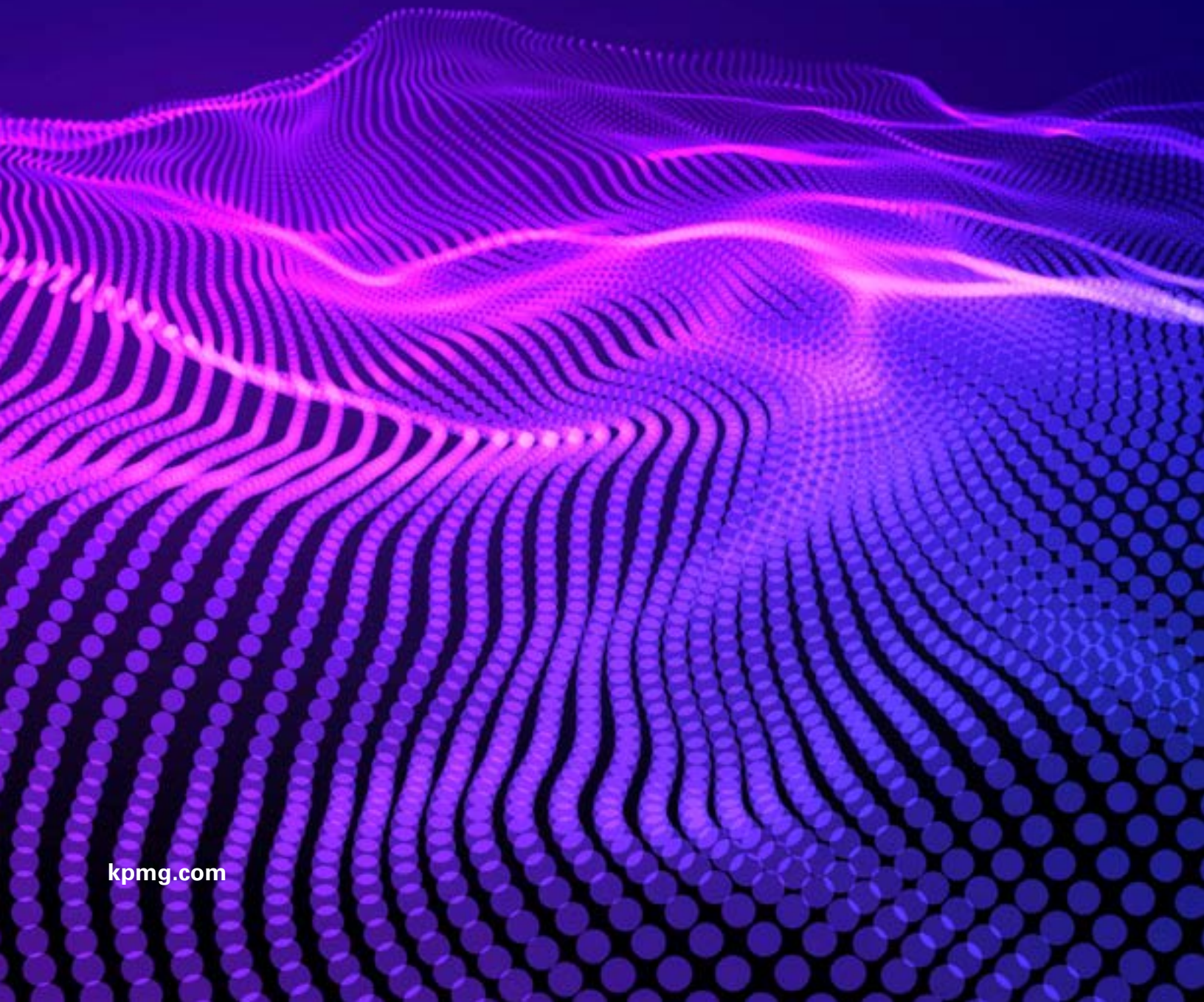
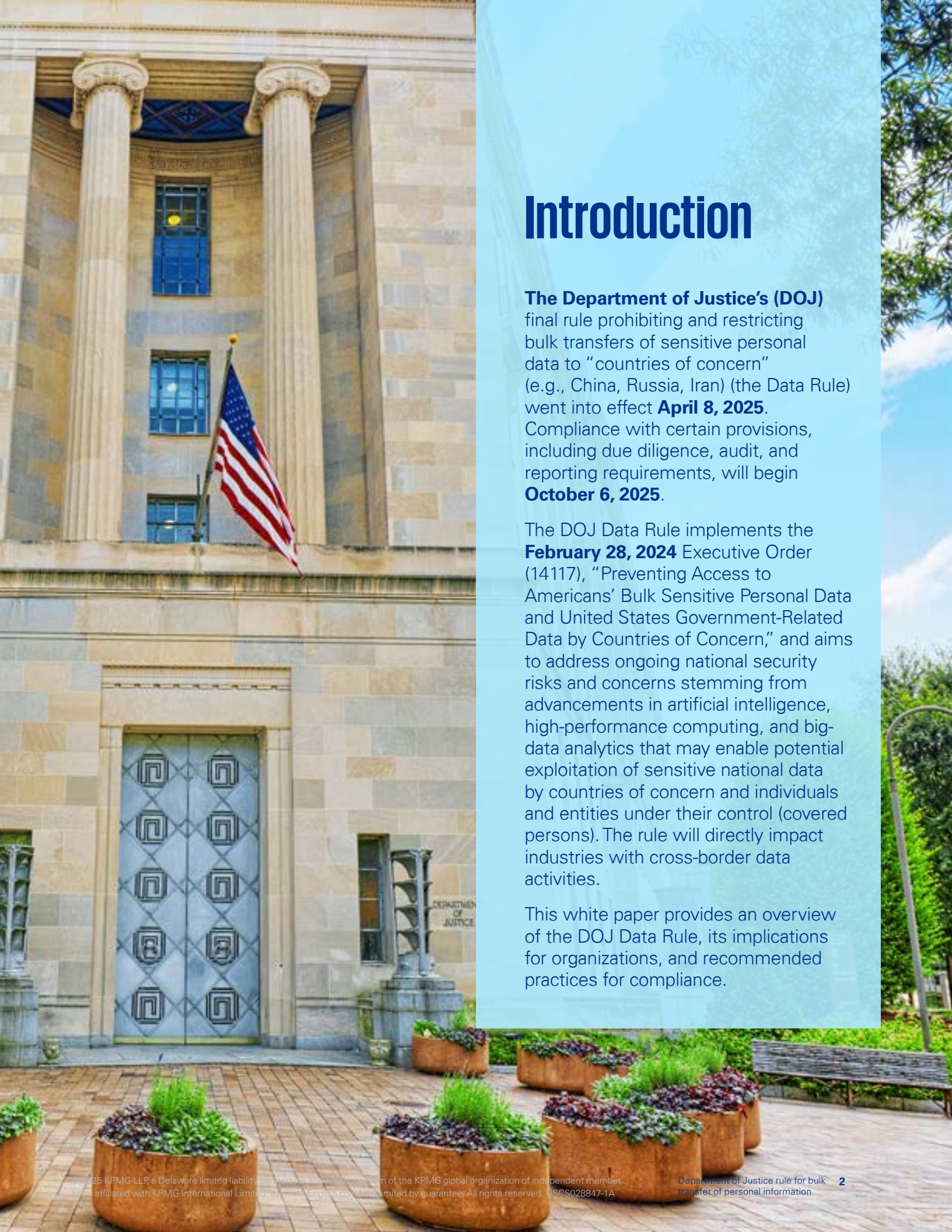
KPMG

Department of Justice rule for bulk transfer of personal information



kpmg.com



Introduction

The Department of Justice's (DOJ) final rule prohibiting and restricting bulk transfers of sensitive personal data to "countries of concern" (e.g., China, Russia, Iran) (the Data Rule) went into effect **April 8, 2025**. Compliance with certain provisions, including due diligence, audit, and reporting requirements, will begin **October 6, 2025**.

The DOJ Data Rule implements the **February 28, 2024** Executive Order (14117), "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," and aims to address ongoing national security risks and concerns stemming from advancements in artificial intelligence, high-performance computing, and big-data analytics that may enable potential exploitation of sensitive national data by countries of concern and individuals and entities under their control (covered persons). The rule will directly impact industries with cross-border data activities.

This white paper provides an overview of the DOJ Data Rule, its implications for organizations, and recommended practices for compliance.

Background and compliance

The DOJ Data Rule regulates transactions involving six categories of sensitive personal data:

- Personal identifiers
- Precise geolocation data
- Biometric identifiers
- Human genomic data (and other types of human 'omic data)
- Personal health data
- Personal financial data

As a result, healthcare, life sciences, biomedical, and research firms are most heavily impacted by the guidance. The rule takes effect 90 days from publication (April 8, 2025), with due diligence, reporting, and auditing requirements taking effect 270 days after publication (October 15, 2025). The rule aims to prevent foreign adversaries from accessing significant volumes of Americans' sensitive personal data and includes countries of concern such as China, Russia, Iran, North Korea, Cuba, and Venezuela. Organizations must implement robust risk management frameworks to assess, monitor, and mitigate risks linked to Information and Communication Technologies (ICTS) supply chains.

Key compliance requirements include:

- Reporting transactions involving ICTS to the Department of Commerce when requested
- Maintaining comprehensive records of ICTS transactions that could potentially fall under the DOJ Data Rule's prohibitions
- Conducting due diligence to identify and mitigate risks associated with the ICTS supply chain.

Striking a balance – Limiting risk and enabling business value

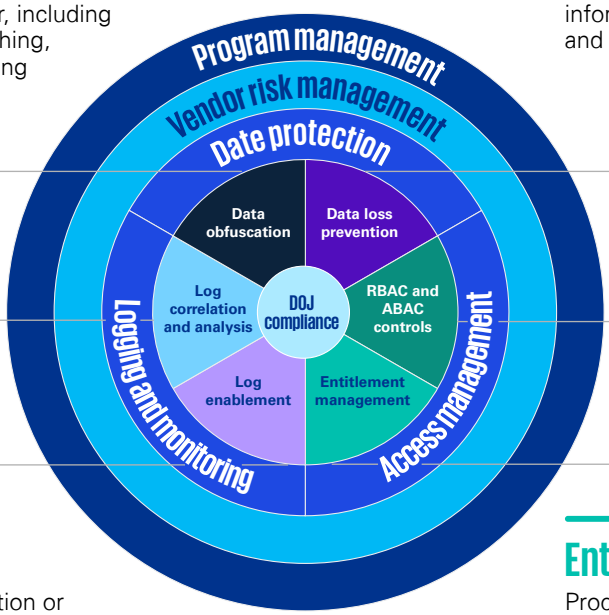
KPMG LLP has developed a proprietary Risk & Compliance Program Framework that integrates US federal guidelines for compliance programs as the foundation and incorporates years of industry experience and guidance from key regulators.

Data obfuscation

Techniques for reducing the value of data if obtained by an unauthorized user, including encryption, de-identification, hashing, variance, substitution, and shuffling

Data loss prevention

Capabilities to monitor and prevent sensitive information during external transmissions and other movement within an organization



Log correlation and analysis

Centralization of collected logs across the organization for performing in-depth security monitoring for unusual behavior and/or activity

RBAC and ABAC controls

Controls for limiting access to a particular file, application, system, and data set based on an end user's job role or a particular attribute (e.g., geolocation, citizenship status)

Log enablement

Generation of logs at the application or endpoint level to track local user activity

Entitlement management

Processes for identifying resource groups, defining policies or access rights, and allowing users to submit requests for access.

Key areas of focus to comply with the rule include:

Data compliance program development: Establish a program management office, governance structure with defined roles and responsibilities, stakeholder groups, and required policy and standard updates.

Vendor identification: Identify and document vendors involved in direct and indirect processing of personal data. This includes vendors and other third and nth parties onshore that may transmit in-scope personal information to countries in question, as well as offshore vendors located in those countries with whom data is shared.

Data flow identification: Identify and document structured and unstructured flows of bulk personal data to in-scope countries. This should capture details around data transferred, technical and procedural controls protecting the data, frequency of transfer, identified risks, and the purpose of the data transfers.

Implementation of technical measures: Implement technical measures required by the Cybersecurity and Infrastructure Security Agency, including multifactor authentication, strong access controls, data masking, encryption, data loss prevention, and other privacy-enhancing controls.

Recordkeeping protocols: Maintain comprehensive records of ICTS transactions and report them to the Department of Commerce when requested.

Annual independent audits: Conduct annual independent audits to ensure ongoing compliance with the DOJ Data Rule and identify areas for continuous improvement.

Why act now?

Implementing effective compliance practices for the DOJ Data Rule reduces risks, improves regulatory compliance, enhances data protection, integrates business processes, and allows for cohesive management of sensitive personal data, among other benefits. A detailed view into a range of the significant benefits that our clients have achieved, as a direct result of adopting the aforementioned leading practices and making significant investments in their compliance programs, is captured in the visual below:

Reduce risks and fines

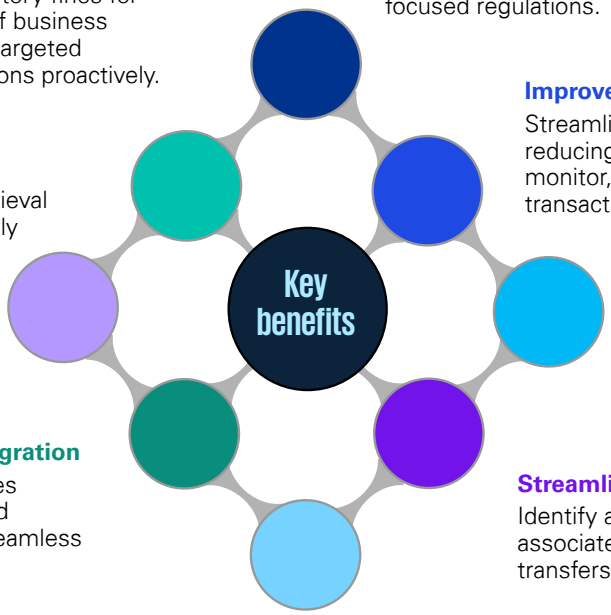
Mitigate risks associated with data breaches, unauthorized access, and regulatory fines for noncompliance. Avoid the risk of business disruption where data flows to targeted countries by addressing obligations proactively.

Enhance data retrieval

Support data availability and retrieval in an accurate, secure, and timely manner to satisfy business needs or for regulatory or legal review while providing a strong foundation for other data-focused regulations.

Deepen business process integration

Align data management practices with corporate infrastructure and business processes, enabling seamless compliance.



Support regulatory compliance

Adhere to DOJ Data Rule requirements, ensuring compliance with identified regulatory mandates, while providing a strong foundation for other data-focused regulations.

Improve efficiency

Streamline data management processes, reducing the time and effort required to monitor, report, and audit sensitive data transactions.

Improve accurate data identification

Enable data across the organization to be accurately identified and assigned retention requirements.

Streamline business processes

Identify and address process inefficiencies associated with cross-border personal data transfers.

Enhance data visibility and management

The activities that support compliance with the DOJ Data Rule are foundational to data governance and protection.

Compliance with the DOJ Data Rule requires an adviser with demonstrated experience

Given the business criticality of compliance with the rule, and implications to noncompliance, it is important to select an adviser that has deep experience in helping companies navigate similar compliance initiatives. We offer a range of services to meet you where you are today as you prepare for your compliance journey.

Our compliance readiness services offer thorough and customizable approaches for organizations to manage complex nuances of data discovery, management, and protection. **We help organizations reduce risk, increase efficiency, align compliance with legal and regulatory requirements, and reduce costs.**

01 PMO build and run

02 Current-state assessment, gap analysis, and detailed roadmap

03 Use case development, requirements definition, and remediation tooling functional design

04 Regulatory responses

05 Hands-on implementation of technical and procedural controls

06 Change management and managed services

Subscribe

Contacts

Orson Lucas

Principal, Cybersecurity & Tech Risk
KPMG LLP

727-480-6623
olucas@kpmg.com

Ellen Ozderman

Managing Director, Cybersecurity & Tech Risk
KPMG LLP

240-750-5669
eozderman@kpmg.com

Gary Rich

Director, Cybersecurity & Tech Risk
KPMG LLP

213-972-4000
grich@kpmg.com

Chris Kypreos

Director, Cybersecurity & Tech Risk
KPMG LLP

415-963-5148
ckypreos@kpmg.com

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

Learn about us: **kpmg.com**