# GDPR Compliance using RSA Archer

## KPMG Point of View

**What is GDPR?** The European Union (EU) General Data Protection Regulation (GDPR) is a law designed to update and unify the EU approach to privacy and data protection. Full text is available at the European Commission Web site (http://ec.europa.eu).

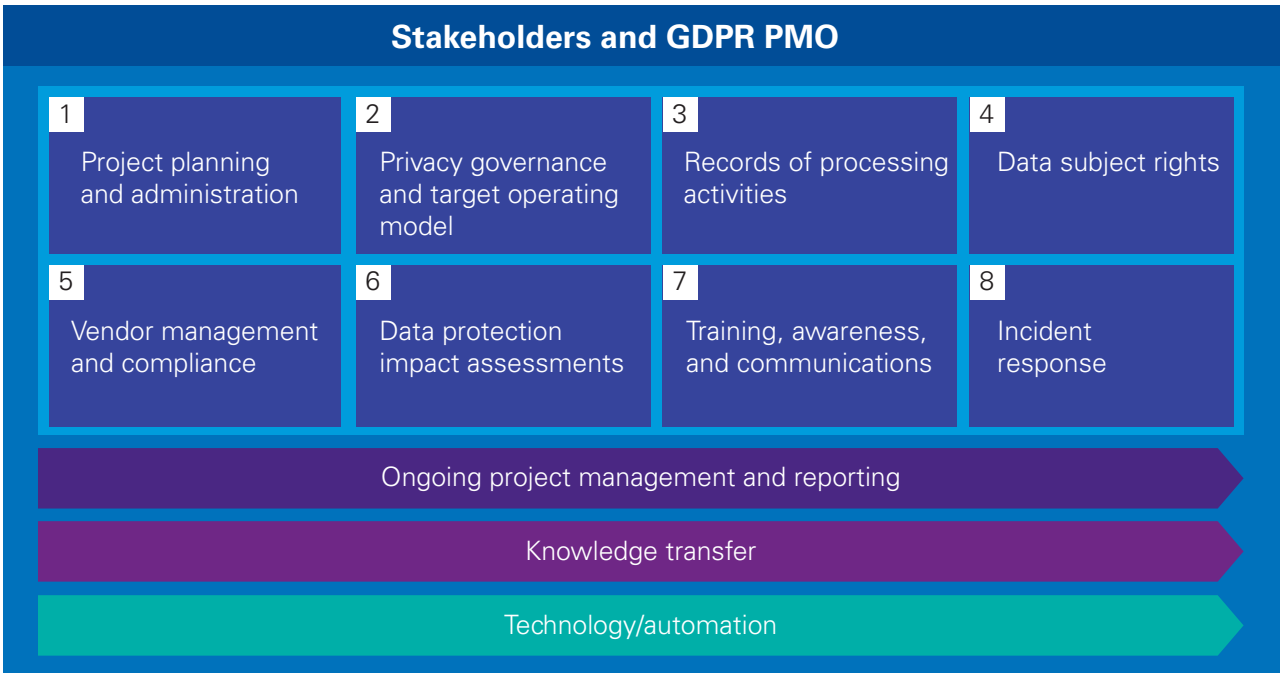
**Where to start?** There is already enough material on GDPR to fill a local library. Most of this information speaks to the onerous nature of the regulation and the investment needed to comply with its many articles and expectations. There is one critical item, however, that this material does not address, which is, *"What do I do first?"*

The simple answer is that impacted organizations must address the five most critical GDPR required actions. These include developing, implementing, and governing the following:

- Privacy governance model
- Records of processing activities
- Data protection impact assessment
- Data subject rights
- Privacy incident response.

**It's all about data, isn't it?** Although it may seem counterintuitive to privacy practitioners, organizations are too focused on and distracted by data when it comes to privacy compliance. In order to sustain privacy compliance and risk management efforts over time, organizations should instead start with an intimate understanding of business processes. With GDPR, the Privacy Office must be familiar with how (and why) high-risk business processes gather, use, manage, and store personal data. Armed with this understanding, the Privacy Office can make better risk-based determinations of where to focus privacy governance investments.

**How can KPMG help?** KPMG is different. We work alongside our clients to design, implement, and govern a self-service, on-demand, and solutions-focused approach to privacy compliance that will demonstrably deliver real business value by materially lowering the cost of compliance, lowering the cost of control, and increasing the confidence that executives have with regards to protecting at-risk personal data assets. Our approach to GDPR readiness is organized via the phases listed below.



**RSA Archer and GDPR**

GDPR compliance efforts are similar to complying to other regulatory mandates. Like other compliance management efforts, technology implementation is an integral component of GDPR enablement. It is KPMG's belief that RSA Archer can be an effective enabler to automate GDPR compliance processes by using RSA Archer's out of the box applications and questionnaire capabilities.

| Archer use case | Application to GDPR program requirements |
|---|---|
| Information Technology (IT) and security policy program management | — Document and centrally store policies, standards, and procedures that support compliance with GDPR requirements<br>— Manage policy life cycle, including policy exceptions and review cycle |
| IT risk management | — Identify and tag business processes and IT assets involved in the handling and processing of EU personal data<br>— Perform risk assessments to identify and rank risks, and link to existing controls<br>— Identify and prioritize high-risk issues |
| IT controls assurance | — Document, assess, and report on GDPR controls<br>— Identify any gaps or issues during controls testing that can be managed through remediation<br>— Report on GDPR compliance through control testing results |
| Third-party risk management | — Manage assessment of third parties to determine GDPR applicability<br>— Manage assessment risk across third parties within scope of GDPR<br>— Inventory issues and remediation |
| Data governance and privacy program management | — Centrally manage processing activities and capture data such as associated regions, countries, data stakeholders, roles and responsibilities, related business processes, Article 30 checklist, external data processors, safeguards, and related issues<br>— Create data protection projects and initiate privacy impact assessments and data protection impact assessments |
| Issues management | — Centrally store and manage findings, remediation plans, and exception requests related to GDPR, leveraging existing risk assessments, control testing, or third-party assessments<br>— Prioritize issues to react more efficiently and reduce risk and cost related to GDPR compliance gaps |

# Contact us

For more information on how KPMG can help your organization build a GDPR-ready program, contact:


**Lokesh Ramani**
**Advisory Managing Director**
**T:** 206-913-4491
**E:** lramani@kpmg.com

**Orson Lucas**
**Managing Director, Advisory**
**T:** 813-301-2025
**E:** olucas@kpmg.com

**Juliet Hodder**
**Alliance Director**
**T:** 510-378-6765
**E:** juliethodder@kpmg.com


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

**kpmg.com/socialmedia**




May 2018