KPMG

Ahead of the curve

Transforming the privacy challenge into competitive advantage

Managing personal data in the wake of GDPR

Personal data is the lifeblood of the digital economy. Yet responses to privacy regulation and to new legislation such as the European Union's General Data Protection Regulation (GDPR) must go beyond compliance. An automated approach to data privacy not only creates a more efficient internal process that requires fewer resources, but also creates competitive advantage on multiple fronts.

Companies with European operations or that otherwise handle the personal data of EU or EU-based customers or employees are subject to the terms of GDPR, regardless of location. Companies the world over rushed to create the minimum viable product (MVP) required to achieve compliance with these new regulations—and many breathed a sigh of relief when the May 25th deadline for compliance had passed. But the real impacts of GDPR are only beginning to be seen.

Organizations now need to set their sights on longer-term goals. Once regulatory compliance has been achieved, the focus needs to turn to operationalizing and automating data privacy processes to create a more effective, efficient response. Through automation, businesses can reduce costs, forge stronger and more responsive customer relationships, and use privacy as a source of competitive differentiation.

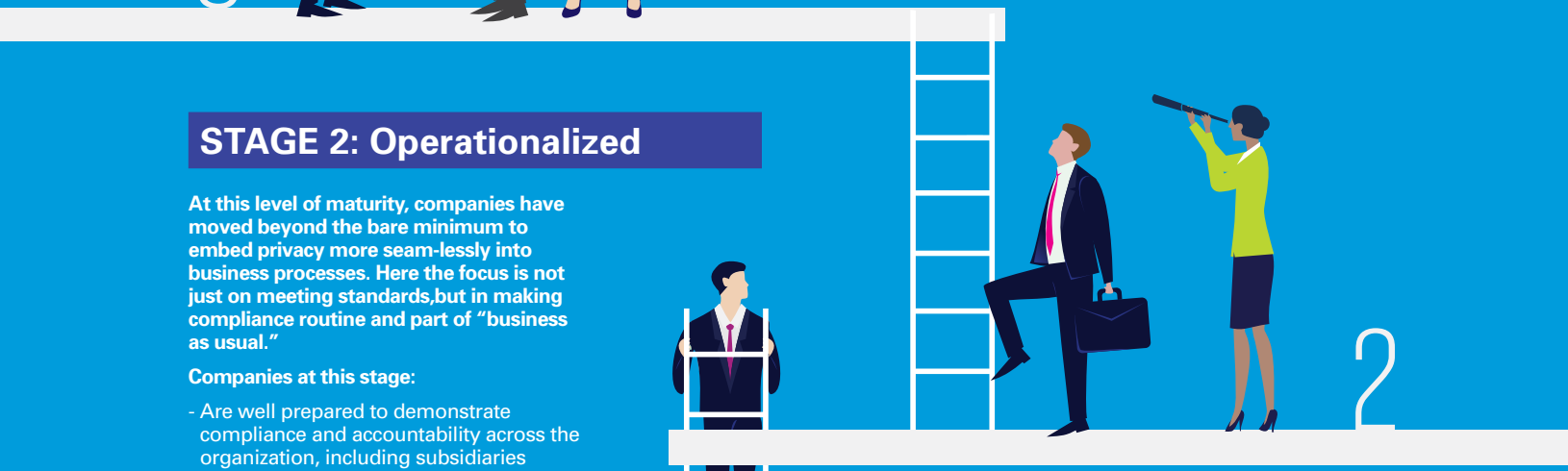
The three stages of GDPR maturity

STAGE 3: Automated

At this level of maturity, companies embrace the technology, tools, and processes needed to automate the work of compliance. Companies at this stage optimize privacy compliance through self-service, on-demand tools to improve speed and efficiency, and use privacy as a differentiator to gain significant competitive advantage.

The goal is to enable the existing technology landscape while integrating additional technology capabilities to address critical gaps. For companies at this level, core areas for automation may include:

- Data identification and classification
- Identity and privileged access
- Privacy and GRC controls
- Encryption and DLP
- Monitoring and response



STAGE 2: Operationalized

At this level of maturity, companies have moved beyond the bare minimum to embed privacy more seam-lessly into business processes. Here the focus is not just on meeting standards,but in making compliance routine and part of "business as usual."

Companies at this stage:

- Are well prepared to demonstrate compliance and accountability across the organization, including subsidiaries
- Quickly and completely respond to regulatory, customer, and third-party inquiries
- Continuously assess, identify, and address potential gaps in compliance
- Look to operationalize compliance change across in-scope business processes
- Begin automation efforts.

STAGE 1: Minimum Viable Product

This level of maturity reflects a posture that supports the minimum required to achieve regulatory compliance. In most cases, this is characterized by a heavily manual or ad hoc approach.

For many companies at this stage:

- The privacy policy and public-facing elements show compliance, but there are gaps in supporting processes.
- The scope of coverage may be limited to high-risk areas.
- Some data subjects may not be covered under established processes and controls.
- Delays in the fulfilment of data subject rights could draw unwanted regulatory scrutiny.

Automating to get ahead of the curve

When it comes to data privacy, going beyond regulatory compliance can offer competitive advantage on three fronts: market differentiation, cost, and responsiveness to customer needs.

For global organizations, all major competitors are required to meet similar standards. Given the costs of adopting even a baseline level of compliance, most companies to date have focused on achieving the bare minimum. Organizations that get ahead of the curve to maintain compliance more efficiently and with less overhead can instead focus resources on other business priorities.

Greater privacy maturity can deliver competitive advantages based on cost. Manual processes can require significant employee time, may require additional dedicated privacy office resources, and likely delay critical technology and business transformational change. Automating parts of privacy compliance (such as parts of PIA reviews, records of processing, privacy contract management, and more) can decrease resource costs while increasing the business's speed to review and enact change.

Meaningfully embracing a new mind-set around personal data can also help achieve differentiation from a customer standpoint. GDPR regulations favor those that embrace the spirit, not just the letter of the law; however, while most organizations now have the necessary policies and procedures in place, fewer stay true to the spirit of the regulation. As enforcement activity begins in coming months, companies that only paid lip service to GDPR compliance will begin to feel the impacts—not only from stiff penalties, but also potentially from the associated customer and public relations fallout from privacy missteps.

Perhaps most importantly, being closely attuned to the voice of the customer can forge deeper, more valuable relationships and help with attraction, retention, and enhanced monetization of the customer relationship. To achieve this, companies need to not only carefully consider how they are handling personal data, but also the ways in which they interact with customers, taking into account the end-to-end customer relationship and experience. Embracing a new mind-set around personal data helps foster a customer-focused culture that can engender greater customer trust. As trust increases, so too can the total volume of data given into the company's care, enabling better understanding of customer needs and improving marketing and outreach efforts.

Help on the road ahead

GDPR compliance is a complex area, and data privacy responsibilities are only expected to grow. For most, privacy may not be a core competency area, but it can be a differentiator if designed and implemented thoughtfully. Today's companies need to get out in front of the curve and proactively build the capabilities needed to create a new steady-state business model.

KPMG Cyber Security Services provides tremendous capabilities to assist organizations to optimize, operationalize, and automate privacy compliance change across the business. With our clients, KPMG coordinates the convergence of privacy, legal, compliance and cybersecurity technology platforms to enable a holistic privacy program. KPMG can help:

– Assess and validate current state and MVP

– Create a business transition plan

– Provide support around enabling technologies

Contact us

Orson Lucas
Managing Director, Advisory
Privacy, Co-Leader
813-301-2025
olucas@kpmg.com

Scot Alexander
Solution Relationship Director
Cyber Security Services
513-421-6430
scotalexander@kpmg.com

Toby Sedgwick
Senior Associate
Cyber Security Services
312-665-3077
tsedgwick@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