KPMG

# Personalized care requires personal data

**GDPR in Life Sciences Reference Card**

Global life sciences organizations are working hard to meet the May 2018 compliance deadline for the European Union's General Data Protection Regulation (GDPR). Despite this awareness and focus, their efforts lack specificity, as there is no industry-specific approach that takes into account its unique strategies and risks. Further, one solution does not fit all, as organizations vary in privacy program maturity and risk tolerance. To help organizations begin to refine their approach to GDPR compliance, this reference card outlines the primary areas on which life sciences organizations should focus.

**How to start?** – There is already enough documentation 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 discussion does not address: What do I do first? The answer is: Develop an approach to GDPR that balances your organization's unique business strategy with the most pressing influences in the life sciences industry today.

**It's all about data, isn't it?** – Although it may seem counterintuitive to privacy practitioners, organizations are overly focused on data when it comes to privacy. In order to sustain privacy compliance and risk management efforts over time, organizations should instead start with an intimate understanding of business processes. This may include operational practices within research and development, human resources, medical affairs, sales and marketing, regulatory compliance, etc. Within these realms, the privacy team must be familiar with how (and why) business units gather, use, manage, and store personal data. Armed with this understanding, privacy teams can make better risk-based determinations of where to start and where to focus in their data protection efforts.

**Pay now or pay later?** – Many life sciences organizations view GDPR as the problem of companies based in Europe. As a result, they may take a bifurcated approach to compliance without realizing that GDPR will soon be the norm worldwide. It is much more effective for organizations to integrate disparate business units through a rationalized and harmonized approach that allows for a single set of privacy policies, procedures, and controls that can be referenced across an entire organization.

It is important to note that taking a united approach will help key functions (e.g., compliance, internal audit, legal, cyber) reduce costs and realize synergies after merger, acquisition, or divestiture activity. Also, higher privacy compliance and change costs are to be expected at first. There is an opportunity to include these costs within restructuring budgets as a one-time expenses and look forward to lower costs as uniform global privacy compliance and risk management capabilities take hold.

**How does GDPR impact ongoing strategic transformation?** – For the last several years, change in the life sciences industry has been seismic. Most organizations are still working through business reorganizations and complex information technology implementations. Adding GDPR compliance to the mix may seem overwhelming. However, no organization should stand up a privacy initiative solely to achieve GDPR or HIPAA compliance, for example. Instead these efforts should be the impetus for growth and performance improvements. Further, failing to comply with GDPR now could jeopardize transformation and growth efforts in the future.

*continued*

**The following summarizes how GDPR could impact critical strategic decisions facing life sciences organizations:**

**Mergers, acquisitions, and divestitures** – Although privacy teams know that data use varies across disparate environments, they must shift their mindset so that privacy compliance strategies are addressed during the M&A process.

This will involve coordination with groups managing business process harmonization, IT consolidation, product optimization, and resourcing. Ultimately, privacy teams should collaborate with the project management office to help design and implement data-sharing and data-transfer agreements for the merged organization.

**Emerging technologies** – Personal data is collected, used and managed via such emerging technologies as Cloud, cognitive and the Internet of Things. As data usage evolves, privacy teams must take care to align their efforts with IT architects, engineers, and operations, as well as business partners and strategic vendors. Policies, procedures, and controls should reflect a *by-design* approach to privacy compliance governance. And, teams would be well advised to consult with procurement, sourcing, and legal teams on contract and clause language that meets updated privacy compliance and risk management expectations.

**Personalized care and attention** – Patient diagnosis, treatment, and care have dramatically improved with the introduction of personalized medicine and value-based outcome expectations for new drugs. The foundation of this paradigm shift is advanced data and analytics. If GDPR restricts the use of personal health information, it will be more challenging for life sciences organizations to target underserved disease states and geographies with new drugs and customized education campaigns. In fact, this is top of mind for many CEOs. According to KPMG's CEO Outlook 2017, 32 percent of CEOs say that achieving customer insights is already hindered by customer data that is low in quality. Therefore, privacy teams should work closely with sales, marketing, and commercial teams to balance patient-focused efforts with data privacy compliance.

**R&D optimization** – As pharmaceutical research and development (R&D) evolves to encompass more far-flung clinical trial sites, GDPR data restrictions will have more and more of an impact on the pace and manner in which drugs are brought to market. In fact, 54 percent of CEOs surveyed by KPMG are already reassessing their global footprint. Restrictions on customer data usage in Europe may cause some to reconsider where they locate operations. Privacy teams should work with R&D teams to redesign their informed consent protocols so that they can conduct effective research studies and still comply with GDPR. And organizations must ensure that third parties that help extend and optimize their R&D efforts also address the impact of GDPR.

**How is KPMG's approach to GDPR different?** – KPMG has more than 300 dedicated privacy professionals who support clients with the design, implementation, and governance of the latest privacy capabilities. KPMG is one of the only firms to offer a self-service, on-demand, solutions-focused approach to privacy that demonstrably delivers real business value. This value is realized by materially lowering the cost of compliance, minimizing the cost of control, and increasing the confidence that executives have when it comes to protecting at-risk personal data assets.

**How KPMG Can Help** – KPMG's Cyber Practice assists organizations from pre-breach to post-breach with an eye to transforming their security, privacy and business continuity controls into business-enabling platforms. Our philosophy is that security is a process and not a solution. Therefore, safeguarding IT networks and sensitive data from electronic attack and exposure is a constant endeavor.

Our teams have significant on-the-ground credentials in the cybersecurity space, having been retained by some of the world's largest organizations in life sciences, healthcare and other industries. Our work runs the gamut from strategy and governance, to large-scale security transformation programs, to a full range of cyber-risk and response services, including on-demand malicious code analysis, host- and enterprise-based forensics, network forensics, threat intelligence, and expert testimony.

## Contact


**Fred Rica**
Principal, Cybersecurity,
973-912-4524 | frica@kpmg.com

**Alison Little**
Principal, U.S. Life Sciences
Advisory Leader
973-912-4611 | jalittle@kpmg.com


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



**kpmg.com/socialmedia**