

HEALTHCARE

THE FUTURE OF DATA PRIVACY:

Key Considerations for Managing the GDPR and Trend of Emerging Global Privacy Regulations

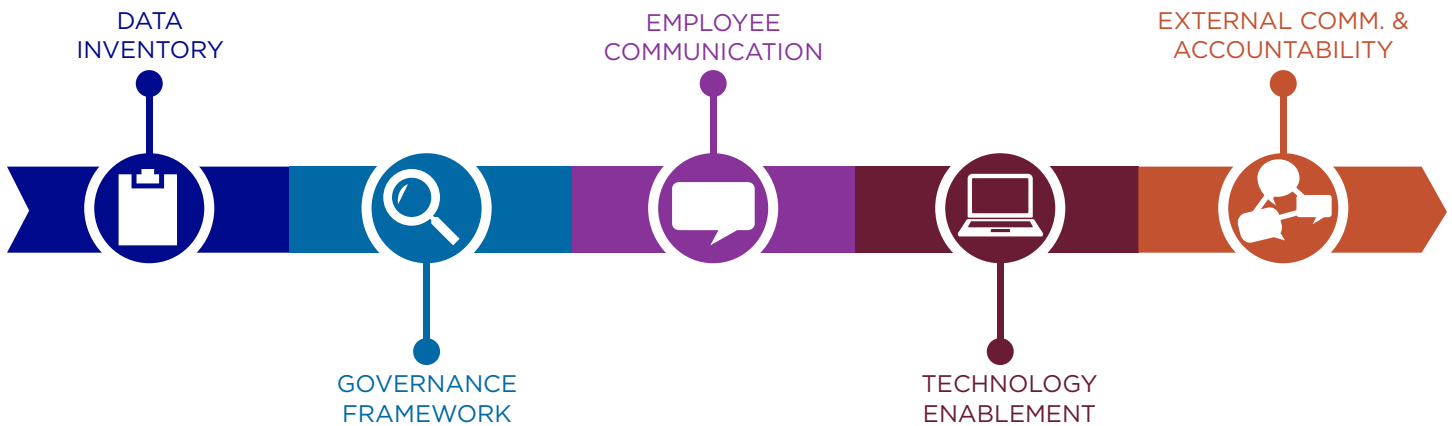
The rise of digital technology continues to advance in such areas as connected health, telemedicine, combination products, the internet, and other customer and employee engagement tools. Yet, while these advancements have proven to provide incredible commercial benefits, they also pose increasing privacy risks.

The European Union's General Data Protection Regulation (GDPR), high-profile cybersecurity breaches, and newsworthy invasions of individual personal data rights have brought privacy to the forefront for both consumers and regulators. As a result, organizations must develop policies, procedures, and documentation demonstrating global compliance that can also be operationalized by employees — all the while continuing to move business forward.

The GDPR established the new standard for data protection, to include requirements of organizations to lawfully process the personal data of individuals, whether they are employees, customers, vendors, or patients. One important consideration with GDPR is that it clearly outlines the fines and penalties for non-compliance, including 4% of the previous year's annual turnover (gross sales) or 20 million euros — whichever is higher. The fines alone have raised the awareness levels of executives and boards of directors on a global scale.

Countries throughout the world — and even states within those countries — are proposing and passing new data protection laws that borrow from, modify, and in some cases add to the GDPR requirements on which they are unofficially based. The California Consumer Privacy Act of 2018 and proposed U.S. Federal data protection standards are examples where these requirements are being extended to U.S. operations.

Following are key considerations for global organizations as they focus on managing the GDPR and other global privacy regulations:



1. **Know Your Data:** The first step to any data governance effort is to better understand the landscape of information the organization collects, including the nature and source of information, location, uses, movement, and retention. A documented data inventory or map provides the baseline for assessing organizational risk and developing relevant policies and procedures to govern the information. The usefulness of these inventories extends beyond compliance, to include legal teams for discovery and case management, information security teams for data classification and protection, and commercial functions and operations for business intelligence initiatives.
2. **Develop a Governance Framework:** Organizations should map activities to the various geographies and requirements to provide the baseline for a risk and gap assessment, as well as the project plan and tracking for activities organizations should prioritize. Where possible, it's important to avoid developing siloed policies that focus on narrow regulations and geographies and can be difficult to operationalize and track. Instead, organizational policies that can be amended to cover new regulations for data protection as they emerge globally should be created.

It is important to note the difference between data privacy and data security:

Data privacy focuses on how a company uses, protects, and shares an individual's personal information, whereas **data security** are the safeguards to secure data from malicious attacks and unauthorized access.

3. **Create and Support a Data Governance Office:** Data privacy cannot be handled by compliance or IT alone. Instead, it should be representative of key functions such as compliance, legal, IT architecture, security, HR, and customer operations, as well as the organization's key geographies. A first step is to train the governance team and have them serve as liaisons to raise issues or concerns to leadership, in addition to pushing out and operationalizing new policies and procedures.
4. **Leverage Technology Where Appropriate:** As new regulations like the GDPR have emerged, the practical first step has been for organizations to develop new policies and procedures, as well as document data inventories and task lists in loosely managed systems like email or spreadsheets. To maintain compliance, organizations should consider where it may be beneficial to use technology to keep centralized repositories of key documentation, task management, and tracking automation so that reporting and audits can be easily supported. There may be existing tools the organization uses that can be leveraged without the need for new purchases, but in some cases the unique needs and level of risk may require new solutions.
5. **Identify Privacy as a Commercial Advantage:** Much like the regulations pushed on global organizations in years past that necessitated a change in operations to meet environmental standards, the requirements of data protection can be costly, burdensome, and difficult to manage. However, just as we now see that being environmentally friendly and a good corporate citizenship are often advertised by organizations and demanded by consumers, it is practical to demonstrate that treating customer and employee personal data with proper care is something organizations can advertise to make them more attractive to do business with or work for.

HOW NAVIGANT CAN HELP

Navigant Consulting, Inc. supports our clients in demonstrating compliance with the GDPR and global privacy regulations through our collaborative expertise in compliance, data management, and security. We provide flexible approaches based on client need in the following areas:

- Data Protection Officer (DPO) as a service
- California Privacy — GDPR, HIPAA, California Consumer, and related privacy assessments
- Data inventory and mapping
- Data protection impact assessments
- Privacy and security training
- Data subject rights management
- Policy and procedure development
- Privacy office advisory and operationalization
- Global governance framework development
- Implementation and management of tools to automate privacy compliance

CONTACTS

J. MARK FARRAR, MSJ, CPA, CFE, CFF

Managing Director
+1.404.575.3800
mark.farrar@navigant.com

BRIAN SEGOBIANO, CIPP/E

Associate Director
+1.312.583.2749
brian.segobiano@navigant.com

AVI MOGHADDAM, BSCS, MBA, CSM, PMP

Associate Director
+1.213.670.3267
avi.moghaddam@navigant.com

STEPHANIE M. LEWKO, CFE

Director
+1.202.973.2458
slewko@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage, and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the firm primarily serves clients in the healthcare, energy, and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

 [linkedin.com/company/navigant-healthcare](https://www.linkedin.com/company/navigant-healthcare)

 twitter.com/navigantHealth

©2018 Navigant Consulting, Inc. All rights reserved. W82857

Navigant Consulting, Inc. ("Navigant") is not a certified public accounting or audit firm. Navigant does not provide audit, attest, or public accounting services. See navigant.com/about/legal for a complete listing of private investigator licenses.

This publication is provided by Navigant for informational purposes only and does not constitute consulting services or tax or legal advice. This publication may be used only as expressly permitted by license from Navigant and may not otherwise be reproduced, recorded, photocopied, distributed, displayed, modified, extracted, accessed, or used without the express written permission of Navigant.