Using Information Governance Tactics to Prepare for the GDPR

FTI CONSULTING™ | TECHNOLOGY

Much like Information Governance ("IG"), preparation for the General Data Protection Regulation ("GDPR") is a cross-departmental concern that requires input from many different groups within an organization, including privacy, compliance, legal, line of business, IT and information security. Similarly, top GDPR requirements relate to other Information Governance initiatives such as data minimization, cloud migration, data mining and disposing of sensitive data. Smart corporations can combine aspects of the two, leveraging IG initiatives along with GDPR preparation to align budgets and achieve data protection and governance goals.

The General Data Protection Regulation goes into effect in May of 2018 and applies to any organization that is a processor or controller of European Union citizen data, yet many multi-national companies are still behind in preparing for compliance. This sweeping regulation requires organizations to meet a wide range of guidelines and prioritize data protection initiatives. For example, a U.S. company, even without European operations or employees, must comply with this regulation if marketing or selling a service to European citizens.

Highlights of the GDPR:

Big penalties

Non-compliance leads to fines of up to €20m or 4% of global annual revenues

Privacy by- design and by-default

Privacy considerations must become part of new product, service, system and process design

Breach reporting

Requirement is mandatory and within 72 hours of breach awareness

The right to be forgotten

Individuals may request that companies erase all data pertaining to them

Data protection officer

Large companies must appoint one to monitor compliance

Privacy impact assessments

Regulators will expect them to occur regularly across multiple operations and business units

GDPR preparedness requires cross-departmental work involving privacy, compliance, legal, line of business, IT, information security and outside counsel and other providers. With just a year remaining to put compliance programs in place, corporations need actionable and efficient strategies to effectively prepare.

Prioritizing GDPR Preparedness

The Ten Most Important Initiatives:

1. **Understand how GDPR impacts your business**
   Recommendation: Conduct a gap analysis and generate a preparedness plan

2. **Determine what data you have, where it is located and how it flows internally and externally**
   Recommendation: Develop a data inventory and run a Corporate Data Assessment

3. **Appoint a Data Protection Officer ("DPO") where necessary**
   Recommendation: Evaluate your organization's requirement for a DPO – do you process and store large amounts of personal data?

4. **Implement a Privacy By Design approach to new systems, services and products**
   Recommendation: Develop a privacy plan and policy when implementing new systems

5. **Document compliance activities**
   Recommendation: Create a defensible record of activities to prepare against future inquiries

6. **Implement and document appropriate security measures**
   Recommendation: Assess and tailor your data security processes in light of the GDPR

7. **Create breach response and notification protocols**
   Recommendation: Make sure policies are in place that reflect the 72 hour notification requirement

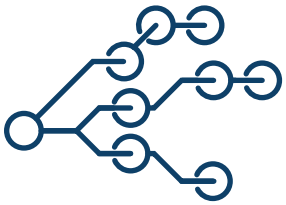
8. **Develop audit capabilities and processes**
   Recommendation: Defensible and documented audit processes can head off questions from regulators down the road

9. **Train and communicate to employees**
   Recommendation: Create an ongoing training & notification program with updates and reminders

10. **Work with stakeholders to ensure budgets are in place to support the changes**
    Recommendation: Use the gap analysis and preparedness plan from item #1 to illustrate importance of GDPR initiatives

Using Information Governance Strategies to help prepare for GDPR compliance:

Much like GDPR preparation, Information Governance is a cross-departmental endeavor and many different groups within an organization share responsibility for it, including privacy, compliance, legal, line of business, IT and information security. Privacy officers, information risk and security officers, IT specialists, counsel, and business stakeholders must work together to ensure information is properly and securely stored, accessed, processed, transported, migrated, retained and/or destroyed. An organization's privacy and security teams are especially key stakeholders whose policies and procedures are critical components underpinning a robust IG program. Given this and GDPR's wide scope, leveraging IG strategies is an effective way to begin moving in the right direction for GDPR preparedness. The following steps are straightforward and achievable ways for corporations to implement effective IG initiatives that will simultaneously help with GDPR obligations.



Data Mapping

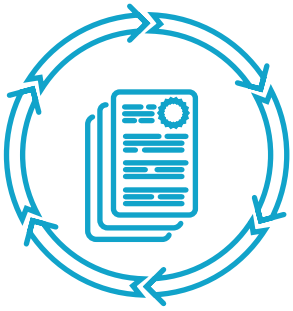
The GDPR includes aspects that are part of the broader IG challenge of understanding the data environment, including what is being housed and where, how it is secured, and the flow of how users access and use it. The GDPR particularly focuses data mapping efforts on personal data, so it is critical to understand the full scope of personal data types that exist in the firm, including the context in which they were collected, their purpose and the legal basis for their usage.

Prioritization of Risk Activities

A best practice in IG is to form a task force of leaders from legal, IT, compliance, the C-suite and other groups to work collectively and holistically to help prioritize areas within the firm which have the most risk from a legal or regulatory perspective – and prioritize remediation efforts. This is also useful for a streamlined GDPR effort, and taking a risk-balanced approach towards remediation is a pragmatic way to deal with limited resources.

Data Remediation

Once data mapping is complete, there may be a need to take action to protect or restrict access to personal or sensitive data. Leverage analytics and machine learning technology and expertise to assist in applying and operationalizing these rules on a larger scale. The same capabilities and expertise can also be helpful in the identification of contracts with third parties where provisions for GDPR need to be reviewed and potentially renegotiated.



Policy and Procedure Refresh

A thorough review of company-wide policies and procedures is another important step. This may include reviewing privacy policies, records management, information security, legal holds, acceptable use, back-up policies and more. Ensure these policies address information obligations holistically with clear roles and responsibilities. With this audit and the data assessment in hand, stakeholders can begin to evaluate which data can be defensibly deleted to reduce the organization's overall storage volumes. Good IG also means creating and maintaining a documented set of repeatable procedures and defensible policies. Under the GDPR there will be a need for updates to guidelines and procedures to handle things like subject access requests, communication to data subjects, consents, data breach disclosure procedures and more. An experienced IG team can help assess current practices in these areas and update in light of the new regulations.

Application Decommissioning/ Retiring Old Systems

When faced with the requirement of searching systems for protected data or for the purpose of erasing data, it's better to have fewer systems to search. The IG tactic of decommissioning old or outdated systems and remediating or migrating the data stored within not only helps with in identifying protected data, but means there will be less of it to search in the future.

Cloud/ Office 365 Migration

As a corporation's cloud strategy develops, legal and compliance teams should be engaged early on to advise on regulatory and legal hold considerations, as well as varying cross-border and security sensitivities. As data processors now also have obligations under GDPR, there will be increasingly complex considerations to meeting GDPR requirements in the cloud. Approach cloud migrations pro-actively with GDPR concepts designed into the process, rather than trying to retrofit requirements later.

IN CONCLUSION:

People and process are key to both IG and GDPR preparation

GDPR preparedness at the core is, like Information Governance, a people and process issue. In fact, the problem most companies face in implementing either is a surfeit of tools, a lack of organizational connectivity and inconsistent integration of process and policy. Truly mitigating the risks involved with GDPR non-compliance will require an enterprise transformation of business processes and technical capabilities that support upstream privacy and security policies, and a cultural shift regarding how personal data should be managed through its lifecycle. With the right resources and expertise in place, organizations can leverage IG and GDPR initiatives to align budgets and achieve data protection and governance goals.

FTI CONSULTING™

www.ftitechnology.com
ftitechsales@fticonsulting.com

North America +1 (866) 454 3905
Europe +44 (0) 3727 1000

Australia +61 (2) 9235 9300
Hong Kong +852 3768 4584

CRITICAL THINKING
AT THE CRITICAL TIME™

About FTI Consulting

FTI Consulting, Inc. is a global business advisory firm dedicated to helping organizations protect and enhance enterprise value in an increasingly complex legal, regulatory and economic environment. FTI Consulting professionals, who are located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges in areas such as investigations, litigation, mergers and acquisitions, regulatory issues, reputation management and restructuring.

www.fticonsulting.com