CORPORATE COUNSEL
An ALM Website
corpcounsel.com | June 14, 2017

Using Information Governance Strategies to Prepare for the GDPR

Sonia Cheng

The General Data Protection Regulation (GDPR) goes into effect in roughly one year, yet many multi-national companies are still behind in preparing for compliance. This sweeping regulation requires organizations to meet stringent data protection requirements over personal data of EU citizens and for the first time, also impacts companies that are based outside of Europe. GDPR defines personal data as any information related to an individual, which can include things like physical address, email address, IP addresses, age, gender, GPS location, health information, search queries, items purchased, etc.

Many companies today freely harvest and commercialize this information. GDPR preparedness involves cross-departmental work involving privacy, security, legal, IT, compliance, outside counsel and other stakeholders. With just a year remaining to put compliance programs in place, corporations need actionable and efficient strategies to effectively prepare.

Feedback from in-house counsel and information governance (IG) professionals around GDPR readiness and urgency has been mixed. In some cases, GDPR has been rated low on the list of concerns that are expected to impact the legal department in the next one to three years. Conversely, respondents in a recent advice from counsel study indicated that GDPR is top of mind for corporations with European operations, customers or partners. The reality of the penalties and litigation risks that may result from noncompliance are serious, and the amount of time corporations have left to prepare is hardly enough for the scope of work that will need to be completed.

Many corporations are struggling with obtaining appropriate funding for the work that is required. Privacy professionals have historically had smaller budgets than counterparts in IT and security. Much like IG, GDPR preparedness requires a cross-stakeholder engagement and involvement from functional stakeholders across IT, marketing,

line of business as well as IT and security. Companies are also challenged with contract renegotiation to comply with enhanced data processing standards. Data controllers and data processors will need to review their data supply chain and ensure that commercial terms are compliant with the GDPR.

Data mapping is another key activity that companies are undertaking to inventory what personal data they have, where it flows, and documenting the legal basis by which they have obtained that information. Some companies have found that partnering with their IG teams to leverage knowledge they already have on what information the company keeps, the retention periods associated with their information and system locations where data resides is a helpful starting point. There are a handful of governance initiatives that can help to accelerate progress, particularly in situations where teams are facing limited budgets and resources.

The following steps are straightforward and achievable ways for corporations to implement effective IG initiatives that will help with GDPR obligations and reducing related risks.

• 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. Existing data maps may not fit for purpose, so it is helpful to quickly identify existing sources to evaluate the level of effort and time it will take to complete the mapping efforts in order to meet the May 25, 2018, deadline.

• Security: IG promotes basic security hygiene in data and also helps to align roles, responsibilities with information access. Security is also a critical aspect of the GDPR. Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. While technological measures are key, companies will also need to ensure that security obligations, breach protocols are refreshed, communicated and employees are trained appropriately.

• Prioritization of risk activities: A best practice in IG is to form a task force of leaders from legal, privacy, security, IT, compliance, the C-suite and lines of business to work collectively and holistically to help prioritize areas or functions within the firm which have the most risk—and prioritize remediation efforts. This is also useful for a streamlined GDPR effort, and taking a risk balanced approach toward remediation is a pragmatic way to deal with limited resources. This prioritization may be regional or functional.

• Data Minimization: One of the core tenants of IG is defensible disposal and encourages companies to keep only what is necessary for business, legal or regulatory purposes. In the past, companies tended to keep things longer as a precautionary measure. With the GDPR, companies are required to change this approach and keep what is minimally required, and delete personal information at the earliest opportunity. The burden of compliance falls on the shoulders of data controllers and processors to demonstrate their process and controls to comply with the GDPR on a consistent basis.

• 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. Companies should consider leveraging analytics, machine learning technology and expertise in applying and

operationalizing these rules on a larger scale. These 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, 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 privacy policies, consent, subject requests, communication to data subjects, data breach disclosure procedures and more. An experienced cross-functional team of internal and external experts are needed to help assess current practices in these areas and update in light of the new requirements.

• 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 redundant, obsolete and trivial data or systems not only helps with identifying personal data, but also means there will be less of it to search in the future.

• Cloud/Office 365: 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.

GDPR preparedness is at the core is a people and process issue. Technology is necessary to help scale the process. GDPR cannot be solved by a magic technology silver bullet. Truly mitigating the risks involved with GDPR non-compliance will require an enterprise transformation of business processes, 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, expertise and capabilities in place, organizations can leverage IG and GDPR initiatives to align budgets and achieve data protection and governance goals.

As senior director at FTI Consulting, ***Sonia Cheng*** *leads information governance initiatives for FTI's Technology practice group, helping corporations deal with the challenges associated exploding data volumes and complying with complex global regulations. Cheng has deep experience in transformation and change across related disciplines in e-discovery, records management, archiving and storage optimization.*