LIFE AFTER MAY 25: What Now?

The GDPR is here.

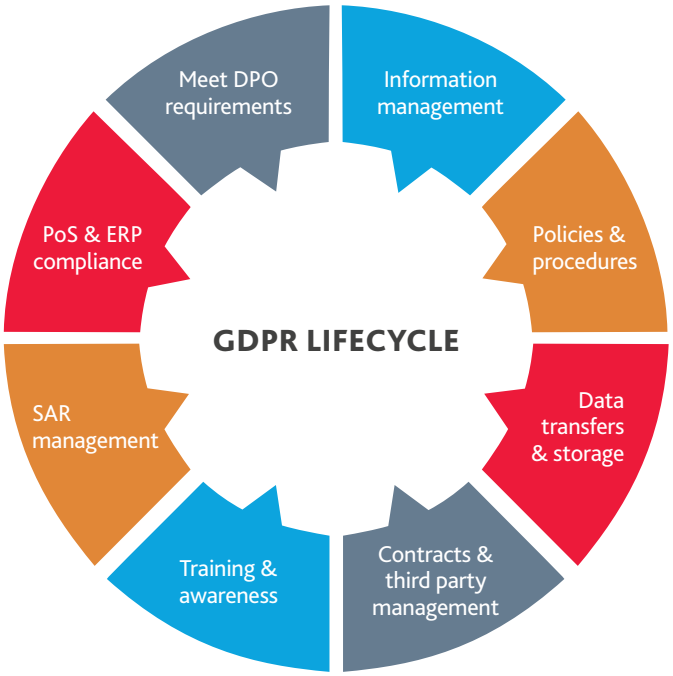
For months, May 25th has been top of mind for companies around the world and now it has finally arrived. Prior to its effective date, the European Union's (EU) unprecedented General Data Protection Regulation (GDPR) has left many organizations wondering how exactly it will be enforced and with what degree of scrutiny they will face, particularly within the first few months. The concern is understandable given the magnitude of potential penalties and sanctions for non-compliance.

Guidelines make it clear that fines can be up to €20 million or 4% of a company's worldwide annual revenue, whichever is greater. Other sanctions that may be imposed either alone or in combination with these fines include penalties like data processing bans or suspension of third country data transfers. Ultimately, sanction decisions will be made by Data Protection Authorities (DPAs) after identifying how the company has failed to meet the regulation and considering what mitigating actions the company has taken to remediate as a result.

While the GDPR has EU personal data controllers and processors fearing strict enforcement, several member state authorities have eluded to providing leniency at the beginning given that implementation of the regulation is currently ambiguous. However, this assumes that the company in question has acted in good faith, taken appropriate action, shown due diligence toward compliance, and has no major flaws in their data protection or information security methodologies.

To minimize immediate exposure, many companies have focused their efforts toward governance and implementation of core capabilities and processes like data privacy policies, consent mechanisms, data subject rights procedures, and secure third country data transfers. While no company can be completely free of risk when processing personal data, it is important under GDPR that organizations log risks found across their enterprise by leveraging tools like the Article 30 Processing Register and Data Protection Impact Assessments (DPIAs), and have taken steps toward mitigating action. Employees should also be made aware of GDPR principles and be required to take training or maintain certifications, particularly in high risk job functions.

The following is one lifecycle to consider when developing your overall GDPR program. Note that not all companies may need to appoint a DPO, but it's at least a question that needs to be asked. Additionally, point-of-sale and ERP compliance may not be necessary for all companies, but it is something to consider and whether automated processes could be implemented for subject access requests (SAR) from enterprise systems. All companies need to consider their information management, policies and procedures, data transfers and storage, contracts, training and awareness, and information security requirements.



BUT WHAT HAPPENS NOW?

While May 25th may seem like the finish line for Day 1 compliance efforts, this is just the beginning. Companies should not only consider enhanced data privacy principles as it relates to EU personal data, but they should implement these standards across the organization, regardless of data subjects' citizenship or country of residence. The reason is two-fold. First, it is a best practice to follow common principles that will satisfy all requirements, typically by complying with the most conservative. It could be overly burdensome to an organization to have to parse data privacy efforts based on jurisdictions. Therefore, companies should leverage the tools required to comply with the GDPR and enhance their governance framework enterprise-wide. Second, it is highly anticipated that many countries will follow the EU's lead with respect to data privacy by reassessing their own privacy laws, if they have not done so already. For example, Canada passed mandatory breach notification as an update to their Personal Information Protection and Electronic Documents Act (PIPEDA). It is clear that enhanced regulations will not stop with the EU, but that we are seeing a global trend to update data privacy protection, largely as a result of modern technology.

For a company to continue on-going diligence it is best to adopt a more proactive approach which will come as a result of operationalizing the GDPR's concept of Privacy-by-Design and Default. Often, privacy is an afterthought for projects, not being considered until the very end, if at all. Under the GDPR, companies must explicitly recognize Privacy-by-Design and Privacy-by-Default, which means they need to incorporate both concepts throughout the project lifecycle. Organizations can leverage this methodology by identifying stage gates that help to satisfy GDPR rules in each phase of product development, software development, IT systems and more.

Life after May 25th is an opportunity to steer away from the reactive approach to the entire information governance spectrum. Adopting a more strategic data privacy framework will bring tremendous benefits to an organization, its business partners, and most importantly its customers.

CONTACT:

TARYN CRANE / Manager
703-770-4441 / tcrane@bdo.com

KAREN SCHULER / Partner
703-336-1533 / kschuler@bdo.com