THE TOP THREE THINGS YOU NEED TO KNOW ABOUT GDPR

The European Union (EU) General Data Protection Regulation (GDPR) enforcement date is fast approaching, with the regulation going into effect on May 25, 2018. BDO's Technology and Business Transformation Services group has been extremely busy over the past year advising and helping clients to assess their readiness for the pending regulation, identifying gaps and working with organizations to define their optimal future state with respect to data privacy, and broader information governance. The consensus is that the focus on these areas will only continue to increase, and that the May deadline doesn't signal a finish line, but a potential starting point or new beginning for how organizations manage their data.

For organizations that either may not have started this journey, or got started a little late, there are three areas that our clients have been focused on in relation to GDPR, right to access, the right to be forgotten, and data breach notification requirements.

1. RIGHT TO ACCESS

Article 15 of the GDPR discusses the right of access by the data subject. To summarize, the right of access means that upon a request by a data subject in the EU, a data controller is required to provide a copy of his or her personal data. (Note: The regulation is not entirely clear if a data subject is a citizen or simply a resident, which may even include temporary residents.) Organizations need to provide several items when responding to this type of request, including:

1. A copy of the personal data that they process (free of charge)
2. The purpose of processing, with a heightened awareness around automated decision making and profiling
3. The types of data being processed (name, address, etc.)
4. Retention periods

One of the first steps in addressing the right to access is performing an assessment to determine how data and information are created, used, managed, and governed throughout the organization. The purpose of this assessment is to evaluate the maturity of how the organization views records and information management, litigation readiness, overall governance and compliance, as well as enterprise information governance (IG). In addition to the assessments, organizations should seek assistance in developing and documenting potential use cases where the right to access might come into effect. Understanding the current state and IG maturity will enable an organization to be prepared for potential requests and position companies to effectively respond. This is a key area for organizations to understand as the deadline approaches.

2. RIGHT TO BE FORGOTTEN

Also known as the Right to Erasure, Article 17 of the GDPR outlines the scenarios where a controller of data has the obligation to erase a data subject's personal data. This has been the primary topic of conversation with clients over the past few months as many are struggling with how to meet this obligation. Operationalizing this activity can often be a challenge for organizations for several reasons. Many times, an organization does not have a clear understanding of where their data is stored. Multiple copies of a file could reside in e-mail, on file shares, on a hard drive, a portable USB device, in a cloud storage solution, the list can go on and on. Many organizations have legal and business requirements to keep data for long periods of time, and other organizations have a culture that encourages "data hoarding". To better understand the data landscape, organizations are creating or updating data maps and application inventories to document how data flows through the organization and who has access to it. Organizations are also leveraging this activity to revisit their data retention policies and schedules, to make sure policies and procedures are current and more importantly, are enforced. Once organizations understand where data is stored, they can build out processes to handle requests and determine what data can be disposed of and how this information can be reported on. Organizations without tight IT controls are at a severe disadvantage, as consumer applications in use in the workplace add complexity to an already difficult problem to solve.

3. BREACH NOTIFICATION

Under Article 33 of the GDPR, breach notification will become mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals". While many organizations may already have a mature breach notification process as part of broader information security programs, the GDPR has a 72-hour notification requirement for when the organization is first made aware of the incident. A coordinated effort needs to be established across multiple stakeholders, including the board, key executives, legal, IT, compliance and lines of business to determine the scope and impact of a breach and what notification requirements apply. Organizations that have less mature processes often start with an **information security assessment** to gauge their readiness.

If you've been tasked with ensuring that your organization needs to be "GDPR Compliant" by May 25, 2018, these three areas are a good place to start.

There are numerous resources available to assist you on this journey including **BDO's GDPR Checklist**. Check with your colleagues in Legal, IT, Information Security, Data Privacy and Compliance to understand what they have done and what they are doing, often their goals and objectives neatly align with GDPR requirements. There is still time to be address these items, but the time to start is now.

CONTACT:

JIM KOZIOL / Director
732-734-3055 / jkoziol@bdo.com

TODD DIETRICH / Senior Manager
713-548-0791 / tdietrich@bdo.com