*Setting a **Higher Level of Excellence** in Information Security & Compliance Services.*

GDPR is coming… but what does it mean, and why should I care?

If your organization hasn't heard these four letters by now, it may not be time to panic - but it is time to learn what they mean and if they could impact organization. Below is a brief overview intended to get you familiar with this new international regulation and hopefully answer some of the basic questions.

What is the GDPR? General Data Protection Regulation - A new set of rules (regulations) established by the European Union (EU) to give its citizens more control over their personal data. This control means organizations must obtain consent from EU citizens for storing and/or using personal data, and such requests for consent must be "explicit," meaning they must be made in plain language and acceptance recorded. EU citizens are allowed to withdraw consent at any time, and individuals have the right to be "forgotten," whereas they may opt to have their personal data removed and/or moved to another organization. The regulation also grants individuals the right to access all data related to them, in an electronic format, free of charge, at any time.

What is Personal Data according to the GDPR? The types of data considered personal according to the regulation includes anything that could identify an individual in the EU (referred to as a "data subject") either on its own or when or combined with other data such as name, address, photos, health information, financial data, IP addresses, web cookies, or social media handles, just to name a few.

Who does the GDPR apply to? It applies to any organization operating within the EU, as well as any organization outside of the EU, offering goods and/or services to data subjects or businesses in the EU. In most cases, an organization will fall into one of two categories: They will either be a "controller," determining the purposes and means of the processing of personal data (e.g. bank) or a "processor," the entity processing personal data on behalf of the controller under the controller's instructions (e.g. a third-party or offsite core system provider). Although the regulation only applies to data subjects while they are in the EU when the data is collected, U.S. organizations should not be too quick in dismissing its applicability until they have fully considered their entire customer base. For example, the regulation would indeed be applicable for organizations with customers who are EU citizens residing temporarily in the United States (e.g. students, frequent travelers, government employees etc.). Another very important point relates to the collection of specific identifying "technical" data, specifically with respect to IP addresses: If an organization collects IP addresses from data subjects in the EU which are then used to market directly to those data subjects, a common practice often enabled through the use of website analytics platforms, then this data would be subject to GDPR. On the other hand, if the same IP addresses are simply collected and no effort is made to directly contact or market towards specific data subjects using this information, then GDPR would not apply.

What is the compliance deadline and what does compliance mean? As of **May 25, 2018**, all organizations are expected to be compliant with GDPR. In a nutshell, compliance means having technical and organizational measures (i.e., controls) in place to protect the security of personal data. Of course, these measures must be documented.

What constitutes a "Breach" under the GDPR? A breach according to GDPR involves unauthorized access to or loss of personal data by a controller or processor and must be reported to the relevant supervisory authority with 72 hours. The supervisory authority according to the GDPR are regulatory authorities established by each EU member country. Note: Not surprisingly it's still a bit unclear as to how such reporting will or would take place.

What are the consequences of non-compliance? Failure to comply with GDPR can result in a fine ranging from €10 mm (approx. $ 12 million dollars) to four percent (4%) of the company's annual global turnover, a figure which for some organizations could mean billions. These figures represent "maximum" enforcement penalties that could be levied

against an organization in response to a significant privacy "incident". It is important to note the actual fine received could be significantly reduced by an organization having reasonable data privacy and due care practices already in place or the ability to demonstrate significant progress achieving such.

Now What? Take a breath, just by reading this far you are in a better position than most, you at least know what GDPR stands for and can begin to assess what it means to you and your organization. Of course, to assess anything requires taking a closer look, GDPR and sensitive data is no exception. If you're thinking *risk assessment* you're absolutely correct. the best place to start in this case is with a Data Privacy Impact Assessment (DPIA). At a high-level, this begins with evaluating the data you have on your current customers (or potential customers you may have directly marketed to) and determine if any are in the EU. Also, if you haven't already, it's probably time to visit the official GDPR website to learn more about the regulation and perhaps take advantage of some of the various data usage scenarios to help determine if GDPR applies to your organization. If, in fact, GDPR applies to your organization, now might be the time to get motivated and begin developing a strategy to assess compliance and close control gaps.

Even if you've determined GDPR doesn't have any applicability to your organization, the spirit of the regulation's intention is the adoption of good information security stewardship and ensuring that risk management programs include organizations' most valuable asset, customer data. What became mainstream with HIPAA in the late 90s has transformed into a focus on privacy oversight in every industry, and is compounded by recent discussions on advertising and social media. That said, implementing some form of GDPR's tenants into your existing programs will not only demonstrate privacy-focused due care for GPDR, but make the burden of implementation much less difficult when/if similar state or federal regulation is mandated.

For community financial institutions, a few focus areas come to mind. While performing a DPIA, consider the following:

- Core Systems – *Who has access to customer information within my core banking platform? For employees, is access assigned granularly to only those with a business need? Does a third-party have access? What controls does the third-party have in place for access by their staff? If a customer were to ask for a copy of all data associated with them, could we provide it? How? Could the data be provided in an easily digestible format? Has my core provider implemented a database structure that accounts for pseudonymization of customer identity with associated data?*
- Document Imaging Systems – *If a customer requests all their data be deleted, does my document imaging solution provide a way for that to be easily done? Can a data deletion request be performed or would that conflict with my organization's Data Retention schedule or other regulatory retention? Is access to customer data within the platform governed by technical controls that support my organization's established Data Classification schema?*
- File Shares and Email Systems – *Does customer data live in shared storage, on servers, and/or local to workstations? Is customer data also in backups and archives? Could I easily remove backed-up and archived customer data without compromising integrity if such were requested?*
- Cyber Insurance – *Is my policy limited to only incidents occurring in the United States or involving US regulators?*
- Web Site – *Does my website use an analytics platform that collects information regarding site visitors? Is it used for direct marketing by yourself or a third party?*

On a final note, while May 25th is fast approaching, there are still many questions surrounding exactly how GDPR is being perceived by U.S. regulatory agencies. As of this writing there has been no "official" comment from U.S. financial regulators on GDPR. Keep in mind, however, regardless of the degree in which GDPR may impact your organization, the

fact remains there is an ever-increasing public concern over data privacy in general, so it's probably a good time to take a fresh look at your organization's data privacy practices. 10-D Security is developing customizable templates to assist with this effort, please contact us, if you are interested.

See for GDPR Regulation: REGULATION (EU) 2016/679