GDPR – How to Get Personal (Data)
By Michael Davis, CISO, CISSP, Cyber zealot

As most know, the European Union's (EU) General Data Protection Regulation (GDPR) was passed into law on May 25th, 2018. The regulation provides significant data protection legislation affecting anyone that might process EU based individual personal data – which is the majority of business entities worldwide. Many organizations have already started their journey to comply with the GDPR, which regulates the security and privacy of an individual's data safety. With this new legislation affecting companies all over the globe, and the recent news of California passing similar restrictions, it's never too late to get started on privacy compliance and better understanding GDPR as it relates to your business.

GDPR – The Basics
Given the significant amount of business done online, it's clear that the GDPR has an international reach. GDPR requirements not only apply to businesses within the EU, they also apply to the processing of personal data of EU residents regardless of company location. It is the location of the person and their data that is important, not their nationality or citizenship. The GDPR's main requirements are that businesses must have full consent and a clear opt-in process from the user.

Consequences for Non-compliance
One reason organizations are not preparing is that they often think the law does not apply to them. For example, it is common for organizations to assume they are exempt if they do not have or process much personal data. Yet, the essential tenet of GDPR is that every business that processes individual personal data of EU residents must comply. Naturally, this leads one to question – what to expect if your organization doesn't comply?

The European Commission provides a four step process (GDPR article 83) before a regulatory entity can impose a fine on organizations for non-compliance. These steps are: (1) Warning, (2) Reprimand, (3) Suspension of Data Processing, and *then* (4) Fines - where the regulation states that sanctions will "in each individual case be effective, proportionate and dissuasive." Therefore, the fine process allows an authority to impose a fine in addition to other mitigation measures.

Compliance Strategies
So what does this tell us? Concentrate on compliance, *not* fines! Don't focus on the punishment – that's just the headline news (e.g., spreading fear, uncertainty and doubt (FUD)) that consultants and companies use as scare tactics to get you to purchase their products and services.

When it comes to compliance, regulatory authorities will focus on two main areas first – transparency (full disclosure to users) and accountability (records and rationale). In addition, you will have to have started implementation with adequate resources for the project – that is, at a minimum you have a plan of action.

You will also need to show an effort at implementing enforcement policies, including:

- Consistency in privacy policies and processes
- Monitoring of sensitive data and select users / accounts
- Clear mitigations when things go awry or get off track

Common Questions
Let's take a moment to briefly address four typical questions associated with GDPR compliance:

Do I need to abide by GDPR?
Yes, you likely will. It's clear that the rules apply unequivocally to everyone who processes EU based personal data. Article 30 states companies with fewer than 250 employees are only required to keep records of processing activities if that could risk an individual's rights or freedoms, or if it pertains to criminal activity. So can you ignore GDPR if you are a small/medium business, maybe - if you can assure your

leadership that neither of those two conditions will ever happen. So what to do? Develop and use a formal GDPR plan, regardless of size, as this shows awareness and intent.

Do I need a data protection officer?
Yes, you might – but likely not. It all depends on the type of data you collect and how much you collect rather than the size of your business. If your processing requires "regular and systematic monitoring of data subjects on a large scale", then you must appoint a data protection officer (DPO). The EU does state that "a group" may employ one DPO between them, as long as the officer is available to all. So what to do?
In short, you will need a privacy advocate. Assign a privacy 'manager/advisor' to be the focal point for your organization and lead the GDPR project.

What about those huge fines vendors extoll?
Organizations can be fined up to 2% of annual turnover or €10 million, whichever is higher, for infractions of the GDPR rules. If there is a data breach with obvious signs of negligence, that fine can grow to 4% of turnover or €20 million, whichever is higher. However, these fines must also be "proportionate", meaning you need to demonstrate (with solid record-keeping and documentation) that your policies and governance framework were built to follow GDPR. Then, if you still sustain a breach, the EU's Information Commissioner's Office (ICO) would be unlikely to levy a significant fine. However, should a data breach occur, the damage to your reputation, trust, brand and market share will be significant in of itself.

Finally, how do I best prepare my company for GDPR?
A solid place to start is the ICO's 12-step guide to preparing for GDPR – tailor it to your needs.
Based on researching numerous sources for GDPR compliance, we propose the following key steps:

- Assess the need for a DPO, assign a privacy liaison at a minimum, and develop a compliance plan.
- Conduct a data audit. Steps for such an audit include figuring out the type of data you process, along with developing a data map, an associated inventory and a risk register to manage the process from start to finish.
- Assess the privacy notices required and associated policies – start with your website notice and draft/update key policies, including: data protection, retention and breach incident at a minimum.

Then, in parallel with the above steps:

- Update your risk assessment (e.g., security of processing article 32). Take a holistic approach to your overall security posture – meaning people, policy, process and product (technology) – using a common framework (NIST CSF, SOC2, ISO27001, COBIT, etc.).
- Implement GDPR education and training – for both employees' overall and data processors.
- Identify your data processors, both internal and external, and conduct third party assessments.
- Update your Data Breach Incident Response plan, providing both contingencies and standard communiqués.
- Review how you ask for consent (if needed) and update that process – be specific and auditable.
- While Privacy Impact Assessments (PIA) are not frequent, develop a PIA and process.
- Understand the 'individual rights' requirements – asses your subject access requests (SAR) process and establish your 'lawful basis', which drives other tasks.

The Bottom Line
Embrace and invest in the GDPR as the global standard it is (which California's new privacy law illustrates), where protecting privacy makes both good business sense and minimizes the risk to your business – be it your company's integrity, brand, market share or profit margin. Leverage GDPR compliance to be a privacy competitive advantage and help future proof your business too.

Mike.Davis.SD@gmail.com