The Open Forum is a vehicle for individuals to provide opinions or commentaries on infosec ideas, technologies, strategies, legislation, standards, and other topics of interest to the ISSA community. The views expressed in this column are the author's and do not reflect the position of the ISSA, the ISSA Journal, or the Editorial Advisory Board.

GDPR – What Does It Mean for Infosec?

By Jason Remillard – ISSA member, Raleigh Chapter

Ah, the land of fear mongering and ranting and raving. GDPR is coming!

Our colleagues in the EU have been subject to this for quite more time than many of us in North America. "GDPR is going to be a huge issue in the coming years" is what a good friend of mine said in 2016. It wasn't until I started researching – I was shocked.

Now, I've been through PIPEDA in Canada. I've been through Sarbanes Oxley in the US. I've seen compliance and privacy programs deployed (some, not so well) worldwide in some of the worlds' largest corporations. I've done GRC modeling in software, whiteboards, and on napkins.

What's the big deal? "Privacy by design" has always been an aspirational goal in many security projects, of course. But how many times have you seen repositories of information no one knew about? How about data taken elsewhere for analysis? Weak (or no) identity and access controls? Little to no encryption?

> *GDPR forces organizations to take very seriously the privacy and access to the information sets they hold.*

How do they force it? With fines of course! Serious, big, large, worldwide fines. "Mess up SOX and people go to jail!" they used to say. Thus far, by my tracking, this hasn't happened yet—even though it was a real risk communicated to all parties.

Now GDPR takes a somewhat different tact, and the Information Commissioner's Office[1] has been very clear, very authoritative, and explicit about the act and its ramifications.

To be clear, in my opinion, the act isn't perfect nor completely explicit in many parts. Somewhat like many of the regs we work to comply with (NIST, ISO, etc.) there is a fair amount of generic guidance in the legislation that leaves some up to interpretation, so there could be some excitement there. When I speak to customers, I liken the GDPR to somewhat like the SOX rollouts that happened in the early 2000s. In the beginning there was much uncertainty, doubt, and confusion. Over time as businesses grappled with the new regulations and worked with regulators, lawmakers, and professionals, it became better defined.

What's been interesting to me is the initial comments like "GDPR doesn't apply to us. We aren't in the UK!" are fading quickly. GDPR is European Union legislation. However, according to a 2017 PwC survey, 92 percent of companies surveyed considered compliance with the GDPR a top priority.[2] That is a BIG number. What worries me more are the organizations that have no preparations. I expect this will be painful for them.

Now, the big day doesn't mean fines will be rolling out that afternoon. Opinion is mixed about what the first days will look like, but a resounding theme is that the legislators won't be deferring anything or exempting segments of the legislation for anyone.

So again, what about infosec? I am seeing that the GDPR will be affecting nearly every application system, data repository, and third-party vendor relationship you have. Much like other regulations, organizations are not able to abdicate their responsibility when it comes to the GDPR, so the onus is directly on the organization to manage its compliance to the legislation. There are many components to the GDPR (access controls, data protection, PII-related and identity remediation, reporting and auditing of capabilities, request interfaces to name a few) with explicit timelines that are challenging for most any organization.

Surely you've had to consider PII and its related information sets in your day to day. The GDPR adds a new lens to those considerations with significantly more material impacts. This new regulation is making the rounds at all levels of organizations and your audit, board, and executive leadership teams should be up to date on it. If not, I would suggest they get started.

For infosec folks who want to understand the impacts? I would ask your friendly local ISSA chapter folks to maybe reach out to legal and professional management consultant resources to come and give some talks. There are many components (99 articles actually!), and information privacy and its management are a business-wide effort. It will involve everyone from application development to customer-facing and vendor management teams.

I hope everyone has started down the path at least a little bit!

About the Author

Jason Remillard, MBA, CISSP, is the President of Data443 and the founder of ClassiDocs.com. He is a founding member of the Blockchain Executive Group and is the former VP of CISO Global Security Architecture and Engineering at Deutsche Bank. He may be reached at jason@data443.com.

1 "Guide to the General Data Protection Regulation (GDPR)," UK Information Commissioner's Office – https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

2 "GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey," PwC – https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html.