RSA Conference 2018

NOW MATTERS

Peer2Peer

35 Days to GDPR. Even If You Prepared, Is Your Firm Truly Ready?

P2P4-T10: 35 Days to GDPR. Even If You Prepared, Is Your Firm Truly Ready?

Ben Rothke, Principal Security Consultant, Nettitude

If regulations are waves, then the General Data Protection Regulation (GDPR) is a tsunami. The GDPR is a European Union regulation on data protection. While other regulations are somewhat limited in what they do, GDPR touches every aspect of data, from the collection, processing, transmittal, application development, data handling and much more. Any firm that handles personal data (and GDPR has a pretty wide definition of what that is) has a lot to do to be GDPR compliant.

On April 17 and 19, I lead two Peer2Peer sessions on the topic at the 2018 RSA Conference. GDPR's go live date of May 25 meant that firms were faced with the reality that they had to be fully compliant. The predicament many attendees were facing was that even with all the preparations they did (and in some cases they weren't all that well prepared), there was still a significant amount of uncertainly if they were doing enough.

The attendees were from a wide range of organizations. Many of them were from US-based firms that have a large presence or headquarters in the EU and did handle in-scope data.

There were a number of areas where the attendees had concerns. The sessions focused on the following areas:

- **Where do we even start?** - "Let's start at the very beginning, a very good place to start" is a line from *The Sound of Music*. But GDPR is so vast, many attendees were struggling to understand just where to start their GDPR work. Do they start at the database, the application, developers, storage, elsewhere?

- **Am I a processor or controller?** – Article 4 of the GDPR creates two very different roles: data controller and data processor. Sometimes a firm is one, sometimes both. But attendees struggled to come to terms with their GDPR identity. Some were hybrid in what they did with personal data. Does that mean that had to do double the effort?

- **Data mapping** – GDPR requires an entity to know exactly where all of their data resides, the data type, and then to classify it. This is a substantial effort that many firms struggled (and are struggling) to complete. An observation shared was that Y2K was about finding every 2-digit year code within application code. That was a huge effort for some firms that had thousands of applications. GDPR is orders of magnitude more difficult as firms need to know the deep dark details of every aspect of PII they acquire and store.

- **Just what is in scope?** – Attendees grappled with defining just what in-scope GDPR data is. There is no conclusive definition of what is or is not considered in-scope for GDPR, and therein lies a huge challenge.

- **Can my company even stay in business?** – We spoke about how Drawbridge divested their advertising business due to the complexities they would have had to gone through to be GDPR compliant. Some attendees questioned how their firms would also be able to comply. (Note that on May 10, 2018 – Klout announced they are ceasing operations on May 25, 2018; which is certainly due to GDPR).

The main theme that emerged is that GDPR is a huge and that the EU regulators are taking it very seriously. Attendees struggled thinking that they are not really sure if they are ready. Many had a lot more questions than we had time for answer. GDPR is going to keep things very interesting.