RSA Conference 2018

Peer2Peer

Practical Planning for the GDPR

P2P1-W04: Practical Planning for the GDPR

Lawrence Dietz, General Counsel and Managing Director, Information Security, TAL Global Corporation

We had quite the full house at the Peer to Peer Session. Delegates came from the US as well as Japan, Italy and Qatar. Industries spanned the spectrum from retail to non-profit to high tech and others.

Our conversations covered a variety of topics. We began by examining what kind of practical coverage the GDPR has. The GDPR is noted for extending protection beyond the borders of the EU and the European Economic Area (EEA) that includes Iceland, Liechtenstein, and Norway.

We noted that personal data about European citizens must be protected regardless of where those citizens are and that any personal data in the EU/EEA must be protected under the GDPR for EU/EEA citizens and non-citizens alike.

Having said that, we discussed that national law governs outside the EU/EEA. As a practical matter organizations must comply with the data protection laws of their own jurisdiction first. Enforcement of the GDPR against overseas potential defendants would likely target big targets first perhaps because many government Supervisory Authorities (Data Processing Authorities or DPAs) are funded by fines.

Another major concern was how the GDPR maps to existing regulations. The GDPR has evolved from the 1995 EU Data Privacy Directive and has included many of the lessons learned by the Member States since that time and the new concerns about Social Media and Data Breaches.

Organizations who are currently following the laws of EU Member States including the UK are significantly ahead of others. However, it is prudent to check key requirements of the GDPR such as the ability to manage Data Subject Requests, Breach notification process and procedures, as well as insuring that the organization understands what personal data it currently has, how it's being used and validating that there is a legal basis behind their personal data usage.

The term 'personal data' is more broadly defined by the GDPR than by other legislation. Essentially it is any data that can identify the individual. "Any" can include visuals such as from CCTV or electronic such as IP address. We discussed how encryption and pseudonymization can reduce risks to personal data.

The magnitude of potential fines, as a share of global revenue has attracted quite a bit of attention considering the high water mark can be as high as 4% of gross national revenue or €20 million or $24 million. The GDPR contains a number of factors that would be used in determining the fine and generally applies the logic of common law that measures intent, gravity of the risk, etc.

The GDPR represents a rare and important pan-European agreement. It appears that many other countries will be following the lead of the GDPR and strengthening their own data privacy laws. The GDPR is a philosophy of privacy by default and design and organizations should consider following it regardless of their location because protection of people's personal data is simply the right thing to do.

Link to references: https://www.dataprivacylaw.com/news/