Insights: Perspectives

5 Key Takeaways | GDPR: Preparing for Meeting with EU Regulators

April 17, 2018

Written by **Jon Neiditz**

KILPATRICK TOWNSEND

5 KEY TAKEAWAYS

GDPR: Preparing for Meeting with EU Regulators

On April 12, 2018, Kilpatrick Townsend hosted the International Association of Privacy Professionals (IAPP) Atlanta KnowledgeNet Chapter Meeting. With more than 80 IAPP members in attendance, **Jon Neiditz** and **Amanda Witt**, co-leaders of the firm's Cybersecurity, Privacy and Data Governance practice, participated on the panel of in-house and outside privacy professionals, which also included Peggy Eisenhauer, Founder, Privacy & Information Management Services – Margaret P. Eisenhauer, P.C.; Aruna Sharma, Assistant General Counsel, Turner Broadcasting System, Inc.; Jonathan Soll, CCO, Network Solutions, Change Healthcare; and David Remick, Partner, KPMG US.

The panel examined important aspects of the EU's soon-to-be-effective General Data Protection Regulation (GDPR). The interactive session began with two mock visits with EU regulators / supervisory authorities (DPAs) during which attendees learned what questions to expect from the DPAs and how to demonstrate GDPR compliance. Following the mock visits, the speakers discussed last-minute preparations to consider before the deadline in order to best demonstrate compliance.

The following are takeaways from the session:

1 The likely reasons that most organizations will find themselves before a DPA will be following a security incident, a data subject complaint, an internal finding following a data protection impact assessment (DPIA) that a high risk activity cannot be mitigated or to simply build a working relationship with an organization's lead regulator.

When meeting with the DPA, preparation is key. Make sure to have all relevant documentation with you in order to establish your compliance with the GDPR. Items that may be needed could include your Article 30 processing register, the relevant DPIA, your incident response policy (if applicable), vendor contracts and diligence, privacy by design policy, etc. Assuming you were required to appoint one, it should be clear to the DPA that your Data Protection Officer (DPO) was involved in all necessary steps of the process. **2**

3 Mock visits / tabletops are key to being fully prepared for the GDPR. Just as you wouldn't want to respond to a security incident for the first time before having practiced your incident response policy, you would not want to meet with a DPA without having prepared for the potential questions you may face.

According to the panelists, Irish Data Protection Commissioner (DPC), Helen Dixon, recently urged companies to be transparent in their practices and disclosures. Organizations should focus on ensuring that individuals' rights to data portability and erasure are respected given that more than half of the complaints the Irish DPC currently receives relate to alleged failures to comply with these requirements. **4**

5

The French supervisory authority, CNIL, will not require the immediate performance of DPIAs for processing activities that have been subject to a prior formality with CNIL before May 25, 2018, or that have already been registered. CNIL stated, however, that for high risk processing activities, a DPIA should be carried out within a reasonable time, which should occur no later than three years from May 25, 2018. Processing activities that have not been subject to prior formalities, that had undergone the required formalities with CNIL but have undergone a substantial change since then, as well as new processing activities taking place after May 25, 2018, require the performance of a DPIA without delay.

For more information, please contact Amanda Witt at awitt@kilpatricktownsend.com

www.kilpatricktownsend.com

Related People

Jon Neiditz

t 404.815.6004

jneiditz@ktslaw.com