ORANGE COUNTY

LAWYER®

OCBA

GDPR: EU GENERAL DATA PROTECTION REGULATION

PHIL MAYNARD, CLO, DISCUSSES COMPLIANCE WITH PRIVACY LAWS

AMERICAN PRIVACY LAWS IN A GLOBAL CONTEXT: PREDICTIONS FOR 2018

PROTECTING THE FOURTH AMENDMENT AFTER *CARPENTER* IN THE DIGITAL AGE: WHAT GADGET NEXT?

WHEN TO ASK, WHEN TO TELL: NAVIGATING CALIFORNIA'S RECENT BAN-THE-BOX LEGISLATION

DATA PRIVACY AND THE LAW

www.ocbar.org AN OFFICIAL PUBLICATION OF THE ORANGE COUNTY BAR ASSOCIATION May 2018 Vol. 60 No. 5 $4.00

PHIL MAYNARD, TEALIUM CLO, DISCUSSES COMPLIANCE WITH PRIVACY LAWS

by COLIN W. FRASER

Data privacy matters more than ever. Big data is revolutionizing the way we do business, as organizations leverage valuable insights to improve services and develop products. At the same time, international privacy laws are taking effect at staggering speed, requiring multi-faceted compliance strategies by organizations engaged in an increasingly global economy. This year is especially important for data privacy because the European Union (EU) will be implementing the new General Data Protection Regulation (GDPR) with wide-ranging consequences even for U.S. companies.

I was able to speak about these new challenges with Phil Maynard, the Chief Legal Officer of Tealium, Inc., a San Diego company with a data-driven business that is ramping up its own compliance with the GDPR and helping customers do the same.

Colin: Hi Phil. To get started, please describe what Tealium does.

Phil: Tealium helps the world's leading organizations manage their customer data across every touchpoint—mobile, web, offline, third-party vendors, and other data sources. We do this by providing a single platform where all customer data is collected, protected, managed, and utilized across the organization, and—in many cases—with third-party technologies, such as email or call center software. Without our technology, companies often take a piecemeal approach to handling customer data that can introduce regulatory risk and lead to poor customer experiences.

What does "privacy" encompass at Tealium? And can you give some examples of data privacy issues dealt with by the company?

As a company focused on helping organizations better manage their customer data, privacy permeates all aspects of life at Tealium. Much of our time this year has been spent ensuring that we can guide our customers, through the use of our services, to meet the data protection and data subject rights requirements of the GDPR. We already have a robust data security program and we are Privacy Shield certified, but the GDPR requires additional measures.

The GDPR requires organizations to demonstrate that technical and organizational measures are in place to ensure the security of the personal data they process. Organizations also must demonstrate ongoing compliance with the GDPR. For Tealium, this meant really understanding our data flows, and conducting data privacy impact assessments and gap analyses. Based on our gap analyses, we implemented measures to protect the personal data in our possession and quickly respond to data subject access requests.

In addition, we have been monitoring the requirements of the EU's ePrivacy Regulation. The ePrivacy Regulation is also expected to come into force in 2018 and will replace the ePrivacy Directive. Because consent with respect to cookies is important to some of Tealium's services, we not only monitor the status of the regulation, but also ensure that when we build products, our privacy-by-design initiatives take into consideration the ePrivacy Regulation.

We have also spent considerable time educating customers. At our 2017 annual user conferences, we dedicated an entire track to data privacy. We also produce whitepapers and webinars that keep customers apprised of regulations that may affect them.

As a data platform company, Tealium is both a data controller and processor, which subjects it to differing privacy frameworks. How does that dual role impact Tealium's compliance efforts?

One role enhances the other. As a data controller, Tealium handles the personal data of its employees and partners who reside in the EU. As a data processor, we handle the personal data entrusted to us by our customers. For example, as a data controller, Tealium responds to "data subject access requests" for visitor data that we collect on our own digital properties such as tealium.com. We offer that same functionality to our customers in our role as data processor. Tealium, as data controller, becomes a "customer" of Tealium as data processor. In building our services with privacy-by-design and privacy-by-default as the foundation, we benefit in our roles as data processor and data controller.

In the United States, data privacy is enshrined in numerous laws, including the Health Insurance Portability and Accountability Act (HIPAA), the Federal Credit Reporting Act (FCRA), and state laws such as the California Online Privacy Protection Act. At the global level, what are the most prominent data privacy laws and why are they significant?

There are several notable data privacy laws coming into force, which become quite striking when you take a step back. These regulations—with the GDPR most top of mind—are establishing a digital bill of rights for the individual. They empower the individual with access to and control over their data, and they require organizations to recognize the responsibility involved in handling customer data.

When it comes to individual laws, the GDPR stands out as one of the most comprehensive, not least because of the potential fines for non-compliance. We also cannot forget the EU ePrivacy Regulation. In addition, we keep up with the data privacy laws and regulations in all jurisdictions where we have customers or employees, including Canada's Anti-Spam Law (CASL), Australia's Privacy Act 1988 as amended, and the Japanese data privacy laws.

One of your responsibilities as Chief Legal Officer (CLO) has been preparing for the GDPR, which takes effect this month. As a U.S. company, why is Tealium subject to European laws governing data privacy?

The GDPR applies to any organization, regardless of where it resides, that either intentionally markets to the EU, or that monitors the behavior of individuals within the EU. Tealium has European employees, vendors, and customers, so we must ensure that we are able to comply with all the requirements of the GDPR, both as a data controller and a data processor.

Not all data is created equal. How do data privacy laws, including the GDPR, categorize various levels of private information to protect the most sensitive components?

You're correct; not all data is created equal and the GDPR specifically recognizes that. Sensitive personal data relates to the fundamental rights and freedoms of the individual. So, any data that reveals health information, racial or ethnic origins, religious or philosophical beliefs, or data about a person's sex life or sexual orientation is categorized as sensitive, and how an organization processes that data could create significant risks to the fundamental rights and freedoms for that individual.

Genetic and biometric data are also special categories of personal data. Such data can only be processed if the data subject gives explicit consent. In addition, Article 87 of the GDPR stipulates that national identification numbers may only be used under appropriate safeguards for the rights and freedoms of the data subject.

Other laws and regulations also differentiate between categories of data. For example, in the US, HIPAA defines the types of personal health information that fall under the regulation.

If an organization complies with the GDPR, which is one of the strictest data privacy laws in the world, will the organization essentially be compliant in all other jurisdictions?

No, not at all. You must still be aware of the laws in other jurisdictions. For example, data residency laws in China and Russia would be key if you intend to process personal data

of Chinese or Russian citizens. The United States has very strong sectorial laws that are on par with, if not more restrictive than, the GDPR, such as HIPAA and Gramm-Leach-Bliley Act. Further, while many member states are enacting the GDPR's measures regarding minors, the United States has long been subject to the Children's Online Privacy Protection Act (COPPA). If you are compliant with GDPR, you are probably in a very good place, but you cannot ignore the requirements of other jurisdictions.

Now that you've gone through the process, what recommendations do you have for other U.S.-based companies preparing for the GDPR's introduction in 2018?

It is never too late to start. View the GDPR as an opportunity to get your privacy house in order. Make sure you create an inter-disciplinary team of individuals who can address data flows throughout the organization and get their buy-in. Get outside help if you have to. This is a big undertaking and, above all else, document, document, document.

We started preparing more than a year ago. We first created an interdisciplinary team that included marketing, human resources, legal, information security, finance, and engineering. That team meets weekly to ensure we continue to gain the expertise of a wide section of the company. We engaged an outside entity to help with our privacy impact analysis, our gap analysis, and mapping our data flows. Once the gap analysis was completed we put together a remediation plan, which included both procedural and technical fixes. We then systematically worked through all the gaps to meet the May 25, 2018 end point.

Will GDPR drive better overall security and privacy practices even for companies that are not required to comply? Do you expect GDPR to raise the bar for security overall?

Yes, and it is a good thing. Companies will not only have to be compliant, they will have to demonstrate compliance, demonstrate employee training, and keep records of processing. This means we are no longer in an era where you can just create a policy and put it in a desk drawer. You now must keep your policies and processes alive and working for you. Consumers are also becoming more aware of their data privacy rights, so companies who commit to better and more transparent privacy practices will be rewarded.

To what extent is the GDPR an opportunity for organizations to increase their market share by attracting partnerships with European companies?

U.S. organizations recognize that the GDPR is addressing a global trend that they, too, will need to address, but it also represents an opportunity to thrive over the long haul in Europe. U.S. companies that embrace leadership positions with respect to data protection, data privacy, and data security will be well-positioned to attract European opportunities. According to recent research by the International Association of Privacy Professionals (IAPP), American companies are taking this opportunity seriously, with 84% of them expected to be GDPR-compliant by May 25, 2018 compared to 72% of EU companies.[1]

> "These regulations—with GDPR most top of mind—are essentially establishing a digital bill of rights for the individual."

How can organizations minimize the business repercussions of complying with international data privacy laws?

The comprehensive nature of the GDPR actually helps with this, as it requires organizations to approach compliance from a holistic, bottom-up approach. One of the principal elements of the GDPR is the concept of privacy-by-design, which requires products and technology that touch customer data to be designed from the start with a focus on protecting privacy. So, instead of regulatory compliance being a checkpoint at the end of the process, it really becomes a cultural shift within organizations to think about this before a single line of code is written.

Our CEO often uses the expression: "People buy into what they help create." That's really what we've seen with this aspect of GDPR. Our engineering team is collaborating with our legal team—not just to comply with the letter of the law, but to conceptualize how we can build future-proofed technology that addresses the needs of the end consumer, regardless of regulation.

With so many laws, so many jurisdictions, and so much change, how is it possible to ensure data privacy compliance? What advice do you have for fellow in-house lawyers working to ensure international privacy compliance?

First off, make sure you are good friends with your information security team. Also, use the GDPR as blueprint for a global privacy compliance plan, not only because it is one of the most comprehensive laws to date, but also because it enshrines many of the personal rights that consumers are starting to expect, regardless of jurisdiction. There are several bills proposed in at least eleven U.S. states that take a page from the GDPR, so even if you aren't focused on Europe, this trend is growing.

But of course, the GDPR is not the only regulation that a global organization needs to focus on; it's important to stay current with the latest information from organizations such as the IAPP and Association of Corporate Counsel. They have wonderful resources available for their members. The data protection organizations themselves are a great resource. For example, the Information Commission Office in the UK is very practical and business friendly. The Office of the Australian Information Commissioner is also very good, and sends email updates on its undertakings. There are also a growing number of privacy law experts that support in-house attorneys.

ENDNOTE

(1) See International Association of Privacy Professionals, "Getting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation," https://download.trustarc.com/dload.php/?f=7QQBJYTO-688.

Colin W. Fraser *is an associate with Greenberg Traurig, LLP in Irvine. He can be reached at frasercw@gtlaw.com.*

This article first appeared in Orange County Lawyer, *May 2018 (Vol. 60 No. 5), p. 26. The views expressed herein are those of the author. They do not necessarily represent the views of* Orange County Lawyer *magazine, the Orange County Bar Association, the Orange County Bar Association Charitable Fund, or their staffs, contributors, or advertisers. All legal and other issues must be independently researched.*