COMMENTARY

4/3/2018
07:00 AM

Kon Leong, president, CEO and co-founder, ZL Technologies
Commentary

Five Traits to Look for in a Data Protection Officer

It's crucial for a data protection officer -- required under the EU's GDPR -- to have a enterprisewide view of an organization's stored data and how it is used, or not used.

Hiring a data protection officer is a vital step in the path towards GDPR compliance, and with the May 25 deadline fast approaching, a step that large organizations are presently beginning to take. Officially responsible for advising on and monitoring the protection and privacy of personal data, this individual will need to successfully navigate several functional, technological, and political obstacles inherent to the role. Let's establish a foundation for hiring a data protection officer by outlining five fundamental characteristics that he or she should have.

Someone who can translate information to many different parties. It's the data protection officer's responsibility to educate the organization on their data privacy responsibilities, as per Article 39. As various departments will use different types of data in different ways and have different pain points for managing that data, a data protection officer must be capable of translating information for each unique case. Whether it's the marketing department analyzing data for competitive advantage or IT trying to store and manage it all, being able to understand each use case and educate the respective party on best practices will be essential.

Someone who realizes the technological challenges. Although GDPR requires extensive procedural changes to business practices, it is by and large a technological challenge. There may be many candidates who understand the regulatory components, but finding a candidate who also understands the technology requirements will be much rarer. There's a long list of questions that few data privacy professionals have considered, let alone have been able to answer. For instance, how does an organization bridge across the many data silos within their organization to search for personal data? How can an organization effectively reconcile policies from various governance functions, such as records management, eDiscovery, FINRA compliance, and GDPR compliance?

A data protection officer who truly grasps the matter at hand will be aware of the technology challenges of GDPR compliance and realize the difficulty of meeting them with traditional approaches to information management.

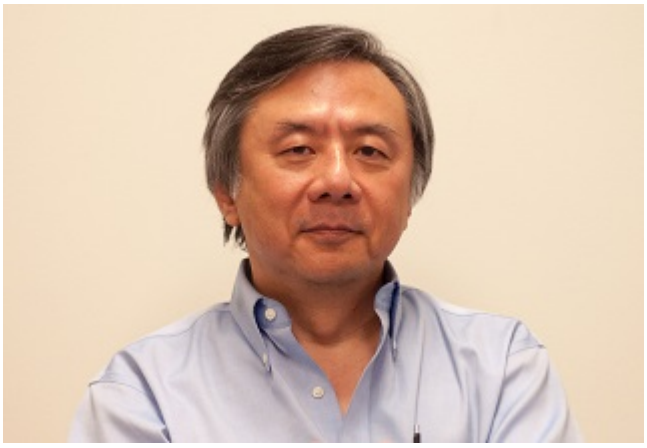
Someone who truly understands data privacy. There are two lines of reasoning when it comes to data privacy. On one end of the spectrum, there is the school of thought that says, "See no evil, hear no evil, speak no evil." In other words, organizations should stay away from personal data and will therefore not infringe on data privacy.

This is not as easy as it seems. If an organization has personal data that they decide to ignore, it becomes impossible to ensure it stays safe. Without knowing what personal data an organization has, they cannot control access privileges, they cannot delete unnecessary data, or quarantine sensitive information.

In fact, it is counterintuitively the most intrusive system that is the most private. An organization must know exactly what personal data it has and exactly how it's being used, so that they can apply the proper restrictions. A good data protection officer will understand this and will therefore work with the rest of your organization to put in place an effective system of information governance.

Someone who understands both the US and EU perspectives on privacy. Whether a data protection officer works for a US company, an EU company, or a company with offices worldwide, they will have to understand that there are massive cultural variations in perspectives towards privacy, which for the most part are divided by the Atlantic Ocean. The US does not have the perspective of having survived several oppressive regimes in the same way that Europe does, which has heightened sensitivity in Europeans towards issues of privacy. It will be important for a data protection officer to fully comprehend these historical cultural differences in order to have an impact on employees from both sides of the pond. Effecting change in American organizations will be fundamentally more difficult due to an inherent naivete towards data privacy. Data protection officers will have to juggle these differences with sensitivity as they speak to different audiences.

Someone who has strong advocacy and diplomacy skills. Because of the nature of the role the data protection officer will in many ways work independently and as an advocate for outside parties, such as data subjects and EU regulators. The data protection officer may be therefore seen as an outsider by some, however they are still responsible for working alongside employees to instill best practices for data privacy. A data protection officer will need the ability to maintain a balance between advocate for the data subject -- oftentimes the consumer or other third party -- as well as a collaborator within the organization. High degrees of tact, diplomacy and integrity will be needed for navigating this uncharted water.



Kon Leong is president, CEO and co-founder of ZL Technologies.

The InformationWeek community brings together IT practitioners and industry experts with IT advice, education, and opinions. We strive to highlight technology executives and subject matter experts and use their knowledge and experiences to help our audience of IT ... View Full Bio

We welcome your comments on this topic on our social media channels, or [contact us directly] with questions about the site.

Related Content Sponsored by

RESOURCES VIDEO

Authenticating The World's Communications

Alexander Garcia-Tobar, CEO, with ValiMail compares email validation much like how a merchant authenticates...

2017 Email Fraud Report

ValiMail's analysis of the most popular 1 million global domains shows that most domain owners have not attempted to implement fraud protection through...

So, You've Started a DMARC Record . . . Now What?

DMARC-enabled email authentication is extremely powerful, but among other this it requires careful configuration of SPF...

An Insider's Guide to Email Authentication Through DMARC

Email is the primary communications medium globally, with over 6.3 billion mailboxes used by 3.7 billion people...

The DMARC Challenge for Federal Agencies

Combining original research and actionable advice this report contains:
Data on how well all 1315 government...

Video

All Videos

Slideshows

Tech Trends: Top 8 Priorities for IT

10 Things You Didn't Know About Soft Skills for IT

15 Best Places to Work in Technology

More Slideshows