CPO Magazine

First Year of GDPR is a Year of Growing Pains With More Pain Than Growth

Sarah Meyer On **May 28, 2019**

Ahead of the one year GDPR anniversary, we spoke with Kon Leong, co-founder and CEO of ZL Technologies, which is an information management provider with clients spanning the Fortune 500, including half of the top 10 financial services companies.

Kon works on-the-ground to future-proof companies against penalties and violations. In this interview, he shares his thoughts on this past year and where he believes the opportunities lie for stakeholders moving forward in being GDPR compliant.

What have we learned in the first year of GDPR?

The first year of GDPR can best be described as a year of growing pains with more pain than growth.

We can all recall the constant updates stating “We’ve updated our privacy policy” plastered across every website and marketing email. While these notices seemingly indicated a change in how organizations approached privacy, if you looked beyond the surface, the technology to support true data privacy and fully comply with GDPR was lacking.

This is still the case. However, despite the technology disconnect, there have been few significant fines as of yet. Regulators have come face to face with the complexity of implementing data privacy in large enterprises, and the reality that we are still years away from being there. And not only do companies have insufficient technology to meet GDPR, regulators also do not yet understand the digital ecosystem enough to properly address fines.

What has been the largest impact of GDPR?

As a result of GDPR and the other regulations that have followed, the convergence of several spaces has been drastically accelerated, with the timeline of this convergence moving up from the next decade to the next few years. Various functions of data management—compliance, eDiscovery, records, privacy, analytics, etc.—and the different types of data—unstructured and structured data, which have traditionally been managed in isolation from one another, now require unified information management. Consider the following scenario: A data subject request his data to be deleted. Can you delete it? No, first you have to check if it's on legal hold. Then can you delete? No, you have to check if it's a business record. And then whether it's needed for other compliance requirements, and so forth. These different areas have been slowly converging, but privacy regulations will necessitate them working in synergy much earlier than expected. In short, the IT architecture of today's silos is "siloed," and GDPR respects no silos.

What can we expect over the next couple years in terms of privacy developments?

Since the release of GDPR, California's Consumer Privacy Act (CCPA) has been the most talked about privacy legislation in America, but other states such as Delaware, New York, and Washington are all developing their own privacy regulations. While they all have similarities, it's their differences that make them difficult to navigate. As states create their own unique privacy policies, the United States will resemble a checkerboard of digital privacy regulations. Because every state's privacy policy has distinct differences, doing business across state lines will become increasingly complex. The technology to manage a single privacy regulation is hardly there, let alone an array of them. A federal privacy law may be forthcoming, but that will come with its own consequences.

Are there any other consequences?

While total privacy may seem like an attractive prospect for end users on the surface, it actually comes with a laundry list of unspoken implications. Perhaps most worrisome of these implications is the paradox that privacy and total intrusion are two sides of the same coin, and it's often hard to tell which side you're on. The fundamentals of privacy are about controlling data all across the enterprise so you can take the required action on them, and that in fact requires extreme insight into data. In other words, every individual's information has to

be completely governed and accessible in order to meet privacy regulations, and once this level of control is available we're only a step away from several dystopian scenarios. Privacy and intrusion are only kept separate by oversight. If oversight is missing, it slips into intrusion. And as a species, have we ever been good at oversight?