COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2021
Increased regulatory scrutiny calls for rigorous data governance

By Bobby Balachandran

Bobby Balachandran (bobby.balachandran@exterro.com) is the founder, president, and CEO of Exterro in Portland, Oregon, USA.

As general counsel and any compliance officer will tell you, COVID-19 has sparked a boom in regulatory scrutiny.[1] There's an incessant flood of internal investigations,[2] employment claims, and corporate audits triggered by pandemic-related workforce reductions, disrupted corporate compliance processes, and dispersed working practices. Added to this are the uncertainties of a slew of new employment regulations; the impact of the California Consumer Privacy Act (CCPA) and its successor, the California Private Records Act; plus the European Union (EU) General Data Protection Regulation (GDPR) directives and a looming federal privacy law for the United States.[3]

Facing these growing compliance burdens, legal teams are of course taking steps to mitigate risk. One of the key strategies to tackle regulatory obligations is building reliable, defensible data management strategies. It's a complex task since organizational data reside in so many different areas with many different data stewards from finance to information technology (IT) to human resources to marketing. Therefore, it is key for legal teams to have the ability to rapidly find and examine data, particularly in response to investigations, litigation, and second requests. Tools, experienced investigators, and forensically sound collection techniques work in harmony to prove that the original data are defensible. This sharpens the focus on data integrity.

Data integrity and defensible data

Each different function in an organization has its own definition of data integrity—enterprise IT thinks about transactional integrity while cybersecurity focuses on the safety of information, and so on. At its core, though, data integrity is an assurance that what was originally created and what people (including investigators) see at a later date remains the same from start to finish. This is the beating heart of defensible data.

The straightest path to data integrity is by instituting processes and workflows that allow information to be collected, searched, and preserved in a consistent fashion. Considering the increasing rate of privacy regulations and compliance mandates related to data security, organizations should take a proactive approach to layer all of the data in a way that is easily searchable and reviewable should a legal issue unfold, such as litigation, second requests, Freedom of Information Act requests, and internal or forensic investigations.

General counsel and compliance officers have to manage an increasingly difficult balancing act between demonstrating governance and compliance, minimizing legal risk, reducing costs, and improving productivity. To help juggle all of this, legal, general counsel, and compliance teams are increasingly turning to single-platform solutions. Why? Varied-point solutions can cost a fortune in time and money, because not only do they have to be managed separately, but there's additional challenge in managing the interplay and incompatibilities between products as they evolve. Therefore, it's far more efficient to use technology platforms that can integrate and orchestrate departmental processes across different workflows, making the data easily defensible and searchable.