COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
Data Mapping: A Necessary Risk Management Tool for Data Compliance

By Desh Urs[1]

Learn how data mapping can help organizations comply with the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other data privacy regulations.

Organizations collect data at a record rate to support everything from improving customer experience to driving operation cost efficiency. As companies collect and process more data, the complexity of managing all the information and ensuring it is secure has also increased exponentially. Simultaneously, there is no end in sight for the proliferation of new international and US state data security laws. Accordingly, boards are asking how the organizations they serve are prepared to deal with these evolving privacy regulations and maintaining compliance with the gowing number of requirements. Unfortunately, the US doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA, to name a few. Currently, California, Colorado, Connecticut, Virginia, and Utah have enacted privacy laws. More than 28 other states have pending or developing data privacy legislation.

To achieve compliance and security, a chief ethics & compliance officer needs to understand their organization's data flow and data management system to adhere to the many privacy laws, safeguard business-critical data, protect their reputations, and avoid hefty penalties.

The Growing Challenges of Keeping Data Safe and Compliant

The rapid adoption of data technologies such as artificial intelligence, Internet of Things (IoT), and cloud-based storage has increased the volume of data and made it harder to know where the data came from and where it is going.

This lack of visibility has increased the risk concerns for many compliance officers regarding their ability to demonstrate compliance with the rules related to the collection, transfer, storage, and destruction. According to a recent survey, 58.6% of the American workforce is working remotely. [2] This dramatic shift in remote working makes it more difficult than ever for organizations to keep track of all the data that passes through or where it is stored inside and outside their systems.

Knowledge regarding your organization's IT infrastructure and how new technologies (e.g., internet of things, data lake, edge computing, 5G, machine learning) are being, or are planned to be, deployed is critical. The first step to gaining this knowledge is to establish an inventory of all the data under your control. You need an inventory that includes what you use the information for, how and where it was collected, where it is located in your data sphere, who has access, and how long you should retain it.

Data mapping gives you the answer to all those questions and more. Besides providing a map for better planning and control, knowing where data is located and used equates to a lowered financial toll should a data breach occur. Breach occurrence has continued to plague both the government and the private sector. This includes the evolution of ransomware strains, much like the COVID-19 virus, that continue to morph and evolve. With a data

map, the impact of a major breach or ransomware event can be reduced by your knowledge and ability to analyze and repond to the event.